Born2beroot

Instrucciones

Ernesto Avedillo

Born2beroot

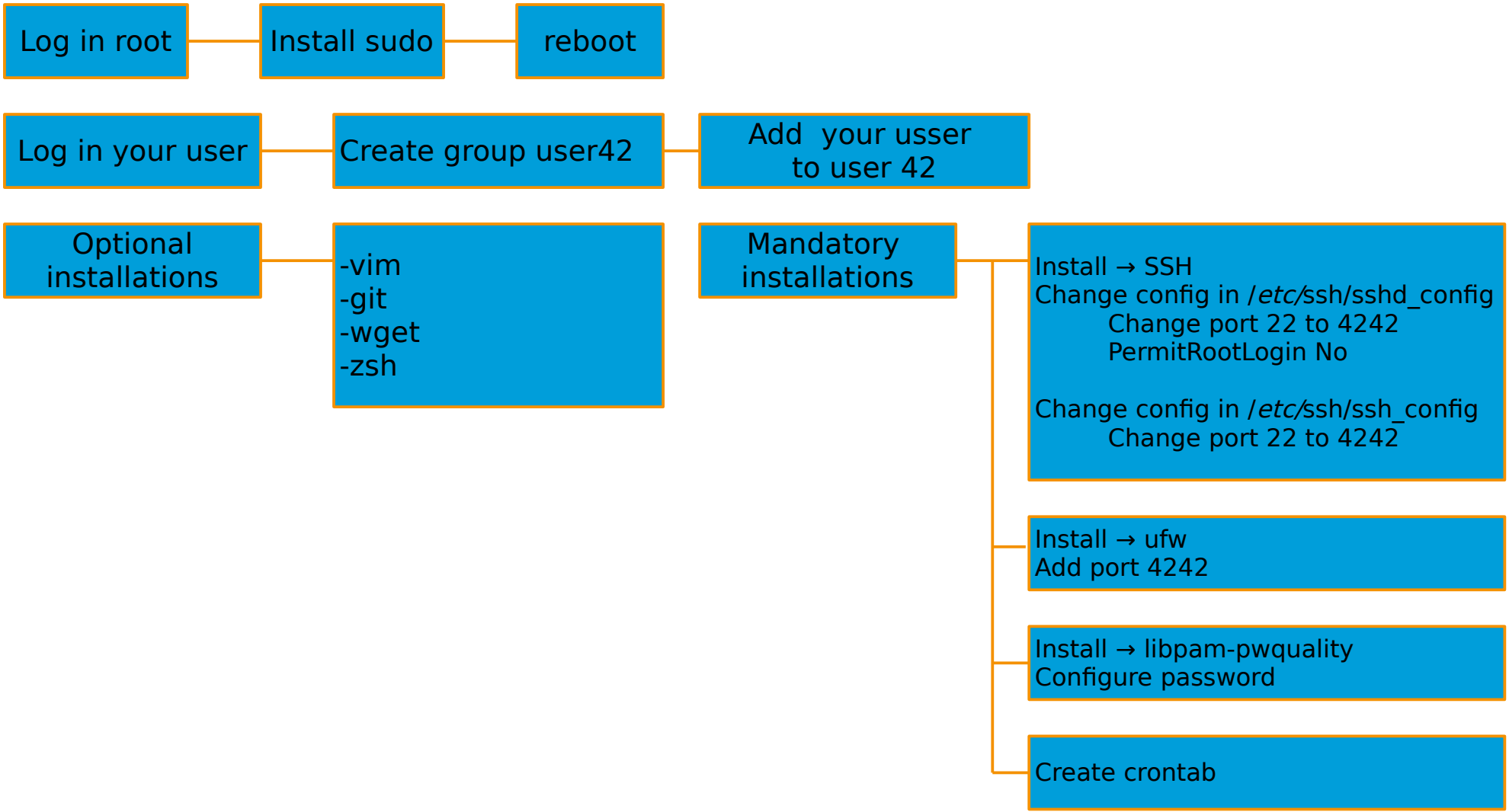
- **Working with users and groups**
  - Listing users → **cat /*etc/*passwd**
  - *Listing groups →* ***cat /etc/*group**
  - Adding users → **sudo useradd -aG <user login>**
  - *Adding gooups →* ***sudo addgroup <group name>***
  - *Assign users to groups:* ***usermod -aG <group> <user>***
  - Check group users → ***getent group <groupname>***
- **General packages to install**
  - **sudo apt install vim**
  - **sudo apt install git**
  - **sudo apt install wget** (needed for onus)
  - **Sudo apt install zip** (needed for bonus)
  - **Sudo apt install bc** (necesario para el monitoring.sh)
  - **sudo apt install zsh** (easy bash system it is optional.
  - **sh –c "$(wget https://raw.github.com/robbyrussell/oh-my-zsh/master/tools/install.sh -O-)"**
  - **sudo apt install build-essential dkms linux-headers-$(uname-r)** (to activate copy paste)
  - **sudo apt install net-tools (used for chrontab)**

Install special packages

- ssh
  - **sudo apt install openssh-server**
  - **sudo service ssh status**
  - **service ssh restart**
  - ***vim /etc/*ssh/sshd_config** → change port 22 to 4242 & PermitRootLogin No
  - ***vim /etc/*ssh/ssh_config** → change port 22 to 4242
  - **sudo service ssh status**
  - **sudo service ssh restart**
  - **ssh <user>@<ipadress> -p port** → to connect with machine
- sfw
  - **sudo apt install ufw**
  - **sudo ufw enable**
  - **sudo ufw status numbered**
  - **sudo ufw allow ssh**
  - **sudo ufw allow 4242**
  - **Sudo ufw delete <number>**

- **Password quality tool**
  - **sudo apt install libpam-pwquality**
  - Edit & modufy ***/ect/pam.d/common-password***

    password requisite pam_pwquality.so retry=3 *minlen=10 lcredit =-1 ucredit =-1 dcredit=-1 maxrepeat =3 reject_username difok = 7 enforce_for_root)*
  - Edit & modify ***/etc/*login refs** (PASS_MAX_DAYS 30 , PASS_MIN_DAYS 2 , PASS_WARN_AGE 7)
  - Edit ***/etc/*sudoers**
    - **Defaults scure path = „…"**
    - **Defaults passwd_tries = 3**
    - **Defaults badpass_message = „Password wrong. Please try again"**
  - Edit ***/var/*log/sudo**
    - **Defaults logfile = „/var/log/sudo/sudo.log"**
    - **Defaults log_input, log_output**
    - **Defaults iolog_dir = „/var/log/sudo"**
    - **Defaults requiretty**
    - **Defaults secure_path = "/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"**
- **Change hostname**
  - **hostnamectl**
  - **hostnamectl set-hostmane <newhostname> --static** (or) **Sudo vim /ect/hostname**
  - **Sudo vim /*ect/h*osts**
    - **127.0.0.1 <localhost>**
    - **127.0.1.1 <newhostname>**
  - **sudo reboot**
- **Chrontab**
  - **Instructions to use to create /usr/local/bin/monitoring.sh:**
    - **uname -a (arquitechture)**
    - **cat /*proc*/cpuinfo (tomar línea physical id and processor)**
    - **free –mega (for RAM)**
    - **df -m (for disk space)**
    - **vmstat (for CPU load)**
    - **who -b (for lst boot)**
    - **lsblk (for lvm existance)**
    - **ss -ta (for TCP connections)**
    - **users**
    - **Hostname -I (for ip address)**
    - **journalctl**
  - **sudo crontab -u root -e**
  - sudo vim **/*usr/*local/bin/monitoring.sh**
  - **sudo reboot**
  - **sudo /*etc/*init.d/cron start**
  - **sudo /*etc/*init.d/cron stop**


Log in root
Install sudo
reboot
Log in your user
Create group user42
Add your usser to user 42
Optional installations
-vim
-git
-wget
-zsh
Mandatory installations
Install → SSH
Change config in /etc/ssh/sshd_config
Change port 22 to 4242
PermitRootLogin No
Change config in /etc/ssh/ssh_config
Change port 22 to 4242
Install → ufw
Add port 4242
Install → libpam-pwquality
Configure password
Create crontab

Install special packages for bonus

- **sudo apt install lighttpd**
  - **Add port 80 (sudo ufw allow 80)**
- **sudo apt install php-cgi php-mysql phpmyadmin**
- **sudo wget htpps//es.wordpress.org/latest-es_ES.zip**
  - **sudo unzip latest-es_ES.zip**
  - **sudo mv html/ html_old/**
  - **Sudo mv wordpress/ html/**
  - **Sudo chmod -R 755 html/**
- **Update & upgrade**
- **wget -O - http://rpms.litespeedtech.com/debian/enable_lst_debian_repo.sh | sudo bash**
- **Update**
- **sudo apt install openlitespeed**
- **sudo /usr/local/lsws/admin/misc/admpass.sh**
- **Add port 7080/tcp 8088/tcp**

Resouestas a preguntas:

- **Preliminarios y General**
  - Asegurarse de que „signature.txt“ está en el repositorio git
  - Revisión shasum
  - Recordar duplicar la MV.
- **Mandatory questions**
  - Como funciona una máquina virtual: Es un entorno donde podemos instalar los SO que deeeemos sin riesgo de afectar la áquina en la que trabajamos. En él podemos instalar un SO antíguo para relizar mantenimientos de programas que todavía trabajan y que no se pueden utilizar con SO mas avanzados. También se puede por ejemplo trabajar en una MV con Linux dentro de un SO de Windows.
  - El sistema operaido elegido el Debian.
  - Diferencias Debian CentOS :

CentOS

Ventajas:

- Sistema mucho mas estable recibe menos updates anuales esto hace que cada uno de ellos esté mucho más testeado. Esto hace que sea mucho ms deseado para aplicaciones industriales.

Desventajas

- Hay que esperar demasiado para las actualizaciones y esto hace que no soorte actualizaciones de versiones mejordas que se revisan con mayor frecuencia. (MySQL)
- Not easy GUI
- Not many apps

APPArmor

- Módulo de seguridad que permite restringir capacidades de un programa.

LVM

- Gestor de volumenes lógicos.Proporciona un método de para asignar espacio a dispositivos de almacenamiento masivo.

DEBIAN

Ventajas:

- Sufre mas actualizaciones por lo tanto es mas fácil que se actualicen los bugs o actualizaciones de niveles de software (MYSQL) o que se adecue a los nuevos avances tecnológicos.
- Many GUI apps.& friendly
- Many apps

Desventajas

- Puede generar mas problemas a la larga.

Diferencias APT y Aptitude

- Aptitude esuna version mejorada de apt APT (Advance Package Tool) ya que gestiona mejor las dependencias entre paquetes de instalacion. Aptitud instala las dependencias recomendadas y apt las requeridas. Aptitud permite congelar instalacion de paquetes (hold) mientras que apt no. Apt integra las funcionalisades de apt-get y apt-cache.

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

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 CentOS and Debian.
  - The purpose of virtual machines.
  - If the evaluated student chose CentOS: 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

Función	apt-get	aptitude	apt
Instalar paquete	apt-get install app	aptitude install app	apt install app
Desinstalar un paquete	apt-get remove app	aptitude remove app	apt remove app
Eliminar un paquete y su configuración	apt-get purge app	aptitude purge app	apt purge app
Actualizar el repositorio	apt-get update	aptitude update	apt upate
Actualizar paquetes (sin eliminar ni reinstalar)	apt-get upgrade	aptitude safe-upgrade	apt upgrade (*)
Actualizar paquetes (eliminando y reinstalando si es necesario)	apt-get dist-upgrade	aptitude full-upgrade	apt full-upgrade
Eliminar dependencias innecesarias	apt-get autoremove	aptitude autoremove	apt autoremove
Buscar paqeutes	apt-cache search app	aptitude search app	apt search app
Mostrar info de un paquete	apt-cache show app	aptitude show app	apt show app
Mostrar estado y candidato de instalación	apt-cache policy app	aptitude policy app	apt policy app
Mostrar las fuentes a repositorios	apt-cache policy	aptitude policy	apt policy
Edición de repositorios fuente	-	-	apt edit-sources
Listar paquetes por criterio	dpkg –get-selections > lista.txt	dpkg –get-selections > lista.txt	apt list
(*) Corresponde a apt-get upgrade --install new-pkgs			

Sudo service ufw status
Sudo service ssh status

Sudo service ufw status
Sudo service ssh status
Groups eavedill
Cat /ect/pam.d/common-password
Cat /etc/login refs
Cat /*etc*/sudoers.d/sudo_conf_login
Sudo useradd <user>
Sudo groupadd <migrupo>
Sudo usermod -aG <migrupo> <user>
Sudo passwd <user>

Hostname
hostnamectl set-hostmane <newhostname> --
static
Sudo vim /ect/hostname
Sudo vim /*etc*/hosts
127.0.0.1 <localhost>
127.0.1.1 <newhostname>
sudo reboot

lsblk

Simple setup

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

- Ensure that the machine does not have a graphical environment at launch. A password will be requested before attempting to connect to this machine. Finally, connect with a user with the help of the student being evaluated. This user must not be root. Pay attention to the password chosen, it must follow the rules imposed in the subject.
- Check that the UFW service is started with the help of the evaluator.
- Check that the SSH service is started with the help of the evaluator.
- Check that the chosen operating system is Debian or CentOS with the help of the evaluator. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

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

Hostname and partitions

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

- Check that the hostname of the machine is correctly formatted as follows: login42 (login of the student being evaluated).
- Modify this hostname by replacing the login with yours, then restart the machine. If on restart, the hostname has not been updated, the evaluation stops here.
- You can now restore the machine to the original hostname.
- Ask the student being evaluated how to view the partitions for this virtual machine.
- Compare the output with the example given in the subject. Please note: if the student evaluated makes the bonuses, it will be necessary to refer to the bonus example.

This part is an opportunity to discuss the scores! The student being evaluated should give you a brief explanation of how LVM works and what it is all about.
If something does not work as expected or is not clearly explained,
the evaluation stops here.

Yes | No

Resouestas a preguntas:

- Check sudo con sudo -V (tambien se puede usar : which sudo or dpkg -s sudo)
- Sudo useradd <user>
- Sudo groupadd <migrupo>
- Sudo usermod -aG <migrupo> <user>
- Sudo passwd <user>
- Sudo /*var*/log/sudo/sudo.log
-

  Para agregar a grupo
- Sudo adduser <user> sudo

- Sudo ufw allow 8080
- Sudo ufw status numbered
- Sudo ufw delete (number

SUDO

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

- Check that the "sudo" program is properly installed on the virtual machine.
- The student being evaluated should now show assigning your new user to the "sudo" group.
- 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. In a second step, it must show you the implementation of the rules imposed by the subject.
- 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. Finally, try to run a command via sudo. See if the file (s) in the "/var/log/sudo/" folder have been updated. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

UFW

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

- Check that the "UFW" program is properly installed on the virtual machine.
- Check that it is working properly.
- The student being evaluated should explain to you basically what UFW is and the value of using it.
- List the active rules in UFW. A rule must exist for port 4242.
- Add a new rule to open port 8080. Check that this one has been added by listing the active rules.
- Finally, delete this new rule with the help of the student being evaluated. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

SSH

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

- Check that the SSH service is properly installed on the virtual machine.
- Check that it is working properly.
- The student being evaluated must be able to explain to you basically what SSH is and the value of using it.
- Verify that the SSH service only uses port 4242.
- 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. It will depend on the student being evaluated. Of course, you have to make sure that you cannot use SSH with the "root" user as stated in the subject. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

sudo crontab -u root -e
/usr/local/bin/monitoring.sh
Sudo /etc/init.d/cron start
Sudo /etc/init.d/cron stop

Lighttpd servidor web
Mariadb es unabase de datos
Phpmyadmin aplicacion web para administrar DDBB
Wordpress istema de gesion de contenidos (FTP)
LiteSpeed software de servidor web

Para entrar en Madirdb:
Sudo mysql -u root -p
SHOW DATABASES;

https://localhost:7080/wp-admin/setup-config.php

Script monitoring

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

The student being evaluated should explain to you simply:

- How their script works by showing you the code.
- What "cron" is.
- How the student being evaluated set up their script so that it runs every 10 minutes from when the server starts. Once the correct functioning of the script has been verified, the student being evaluated should ensure that this script runs every minute. 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. 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. If something does not work as expected or is not clearly explained, the evaluation stops here.

Yes | No

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)

0