

# **PRÁCTICA FINAL ADMINISTRACIÓN DE SISTEMAS**

**2023/2024**

Luis Goenaga Prieto -70910833Q

1.Introducción.....	2
2.Maquina Inicial.....	2
3.Servidor SSH.....	2
4.Servidor Web.....	4
5.Gestion de Usuarios.....	8
6.Directorio skel.....	9
7.MariaDB.....	9
8. Quotas.....	10
9.Cron.....	11
10. Correo.....	12
11. Wordpress.....	13
12.Moodle.....	15
13.Scripts.....	17
14.Aspectos de seguridad.....	18
15.Sftp.....	19
16. Html.....	20
17.Bibliografía.....	22

## 1.Introducción

El objetivo de esta práctica es desarrollar un servidor LINUX para realizar todas las funciones básicas que debe hacer un servidor. Explicaré los pasos en este informe.

## 2.Maquina Inicial

Primero he instalado una máquina virtual de Debian, en concreto la versión 10 (buster). He realizado una partición del directorio /home para separar el almacenamiento de cada usuario, y separarla del almacenamiento que controla toda la funcionalidad del sistema. Empezamos haciendo un apt update y un apt upgrade para estar al día de los paquetes disponibles. Para esta configuración inicial de la máquina hacemos apt install build-essential, que nos incluye algunos paquetes usados generalmente. Luego instalamos una serie de herramientas que forman la base de trabajo en red, con el paquete net-tools.

Posteriormente, para cambiar el hostname y el mensaje al iniciar, hacemos estos dos comandos, previamente instalando el paquete toilet. Con este paquete podemos personalizar el mensaje del día, de esta forma, **toilet --metal GPSystems >/etc/motd**

Para el hostname hacemos **echo "GPSystems" >/etc/hostname**

De esta forma ya tenemos la máquina bien configurada y podemos empezar a trabajar en nuestro servidor.

## 3.Servidor SSH

He decidido usar la opción de ssh debido a que es una opción segura que cifra al completo los datos intercambiados. La seguridad ha supuesto un aspecto importante para elegir esta opción.

Hemos cambiado algunas opciones para mejorar la seguridad

- Puerto predeterminado: Por defecto el puerto determinado del servicio ssh es el 22. Decidí cambiarlo ya que si un atacante intenta hacerlo por este medio, con esta medida le costará más atacar ya que no sabrá el puerto predeterminado.
- Tiempo de gracia de cada usuario, a un minuto.

- Número máximo de intentos, de 6 a 3.
- Desactivamos el login como root mediante ssh.

Una vez hechos estos cambios reiniciamos el servicio con **systemctl restart ssh.server**.

```
gpsystems@GPSystems:~$ su -
Contraseña:
root@GPSystems:~# apt install openssh-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
openssh-sftp-server
Paquetes sugeridos:
molly-guard monkeysphere rssh ssh-askpass ufw
Se instalarán los siguientes paquetes NUEVOS:
openssh-server openssh-sftp-server
0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 398 kB de archivos.
Se utilizarán 1.613 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [5/n] s
Des:1 http://security.debian.org/debian-security buster/updates/main amd64 openssh-sftp-server amd64 1:7.9p1-10+deb10u4 [44,9 kB]
Des:2 http://security.debian.org/debian-security buster/updates/main amd64 openssh-server amd64 1:7.9p1-10+deb10u4 [353 kB]
Descargados 398 kB en 0s (2.981 kB/s)
Preconfigurando paquetes ...
Seleccionando el paquete openssh-sftp-server previamente no seleccionado.
(Leyendo la base de datos ... 147036 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../openssh-sftp-server_1:7.9p1-10+deb10u4_amd64.deb ...
Desempaquetando openssh-sftp-server (1:7.9p1-10+deb10u4) ...
Seleccionando el paquete openssh-server previamente no seleccionado.
Preparando para desempaquetar .../openssh-server_1:7.9p1-10+deb10u4_amd64.deb ...
Desempaquetando openssh-server (1:7.9p1-10+deb10u4) ...
Configurando openssh-sftp-server (1:7.9p1-10+deb10u4) ...
Configurando openssh-server (1:7.9p1-10+deb10u4) ...

Creating config file /etc/ssh/sshd_config with new version
Creating SSH2 RSA key; this may take some time ...
2048 SHA256:FKRHX3ABw70B7avlyYb6GIREDL9RxpI/rcU7ok root@GPSystems (RSA)
Creating SSH2 ECDSA key; this may take some time ...
256 SHA256:8nV4fhCoApkHGsMvU1U57Rlq+Jk/k0kvcyXBjLZImM root@GPSystems (ECDSA)
Creating SSH2 ED25519 key; this may take some time ...
256 SHA256:dgMHyZEwsVNNnQAz9ye+3V4UZP7YfHg3pT7TkFvMufo root@GPSystems (ED25519)
Created symlink /etc/systemd/system/ssh.service → /lib/systemd/system/ssh.service.
Created symlink /etc/systemd/system/multi-user.target.wants/ssh.service → /lib/systemd/system/ssh.service.
rescue-ssh.target is a disabled or a static unit, not starting it.
Procesando disparadores para man-db (2.8.5-2+deb10u1) ...
Procesando disparadores para systemd (241-7-deb10u1) ...
root@GPSystems:~# █
```

```
# $OpenBSD: sshd_config,v 1.103 2018/04/09 20:41:22 tj Exp $

# This is the sshd server system-wide configuration file. See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/bin:/bin:/usr/sbin:/sbin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented. Uncommented options override the
# default value.

#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#LogLevel INFO

# Authentication:

#LoginGraceTime 1m
#PermitRootLogin prohibit-password
#StrictModes yes
#MaxAuthTries 3
#MaxSessions 10
```

## 4.Servidor Web

Usando Apache2, servidor web de código abierto que nos permite mostrar nuestro contenido.

Lo instalamos con **apt install apache2**

```
root@GPSsystems:/etc/ssh# apt install apache2
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  apache2-data apache2-utils
Paquetes sugeridos:
  apache2-doc apache2-suexec-pristine | apache2-suexec-custom
Se instalarán los siguientes paquetes NUEVOS:
  apache2 apache2-data apache2-utils
3 actualizados, 3 nuevos se instalarán, 0 para eliminar y 0 no actualizados.
Se necesita descargar 655 kB de archivos.
Se utilizarán 1.990 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
Des:1 http://security.debian.org/debian-security buster/updates/main amd64 apache2-data all 2.4.38-3+deb10u10 [165 kB]
Des:2 http://security.debian.org/debian-security buster/updates/main amd64 apache2-utils amd64 2.4.38-3+deb10u10 [237 kB]
Des:3 http://security.debian.org/debian-security buster/updates/main amd64 apache2 amd64 2.4.38-3+deb10u10 [252 kB]
Descargados 655 kB en 0s (3.209 kB/s)
Seleccionando el paquete apache2-data previamente no seleccionado.
(Leyendo la base de datos ... 147062 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../apache2-data 2.4.38-3+deb10u10_all.deb ...
Desempaquetando apache2-data (2.4.38-3+deb10u10) ...
Seleccionando el paquete apache2-utils previamente no seleccionado.
Preparando para desempaquetar .../apache2-utils 2.4.38-3+deb10u10_amd64.deb ...
```

Luego he añadido algunas funcionalidades para tener mayor seguridad como el plugin suexec, que se instala con **apt install apache2-suexec-custom**.

Después, añadiremos una capa extra de seguridad a la encriptación de los datos SSL mediante el protocolo HTTPS que es una evolución de HTTP. esto se consigue realizando los siguientes pasos:

**apt install openssl ,a2enmod ssl , a2enmod rewrite** y reiniciamos el servidor apache con **systemctl restart apache2**

Luego modificamos el archivo `/etc/apache2/apache2.conf`, añadiendo estas tres líneas

```
<Directory /var/www/html>
```

```
    AllowOverride All
```

```
</Directory>
```

```
<Directory />
```

```
    Options FollowSymLinks
```

```
    AllowOverride None
```

```
    Require all denied
```

```
</Directory>
```

```
<Directory /usr/share>
```

```
    AllowOverride None
```

```
    Require all granted
```

```
</Directory>
```

```
<Directory /var/www/>
```

```
    Options Indexes FollowSymLinks
```

```
    AllowOverride None
```

```
    Require all granted
```

```
</Directory>
```

```
<Directory /var/www/html>
```

```
    AllowOverride All
```

```
</Directory>
```

Ahora, creamos un directorio para almacenar el certificado ssl, con `mkdir /etc/apache2/certificate`. Accedemos a él y escribimos el comando que se ve en la siguiente imagen. Esto es opcional pero por comodidad lo he hecho así.

```

root@Gpsystems:/etc/apache2/certificate# openssl req -x509 -nodes -days 365 -new
key rsa:2048 -keyout /etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/
apache-selfsigned.crt
Generating a RSA private key
.....
.....+++++
.....+++++
writing new private key to '/etc/ssl/private/apache-selfsigned.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:ES
State or Province Name (full name) [Some-State]:Salamanca
Locality Name (eg, city) []:Salamanca
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:Gpsystems
Email Address []:GPSysmts09@gmail.com

```

Una vez hecho esto, modificamos el fichero /etc/apache2/sites-enabled/000-default.conf, añadiendo las rutas del certificado SSL , que si hemos hecho bien el paso anterior las tendríamos en /etc/apache2/certificate.

```

<VirtualHost *:443>
    ServerName www.gpsystems.es
    ServerAdmin webmaster@localhost

    SuexecUserGroup webadmin webadmin
    <Directory "/usr/lib/cgi-bin/">
        Options +ExecCGI
        AddHandler cgi-script .cgi .pl
        AddHandler default-handler .css .png .jpeg .jpg
    </Directory>

    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # Configuración SSL
    SSLEngine on
    SSLCertificateFile /etc/apache2/certificate/apachecertificate.crt
    SSLCertificateKeyFile /etc/apache2/certificate/apache.key

    # Otras configuraciones específicas para SSL si es necesario
</VirtualHost>

```

Ahora, ya que hemos instalado el suexec, aprovechamos para añadir una pequeña capa de seguridad y hacemos que los archivos cgi de código los ejecute un usuario distinto a www-data. Para ello tenemos que crear nuestro usuario específico para esto.

Con el siguiente comando añadimos el usuario gyermo **adduser --system --home /empty gyermo --shell=/bin/false**

Ahora establecemos una contraseña para el

**passwd gyermo**

**compu.**

Le asignamos un grupo principal y le añadimos a shadow y gyermo

Creamos el grupo gyermo con gid 232->**groupadd -g 232 gyermo** .

Se lo asignamos como grupo principal ->**usermod -g gyermo gyermo**

Le añadimos al shadow, así puede gestionar las altas y bajas de usuarios-> **usermod -a -G shadow gyermo**

Le asignamos al grupo root para que tenga permisos ->**usermod -a -G root gyermo**

Modificamos el archivo `/etc/sudoers` , y le damos todos los permisos con `ALL=(ALL:ALL) ALL`

```
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults      env_reset
Defaults      mail_badpass
Defaults      secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
gyermo  ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#include_dir /etc/sudoers.d
```

Y ahora con **chmod g+w /etc/group** , **chmod g+w /etc/shadow**, **chmod g+w /etc/gshadow**, **chmod g+w /etc/passwd**, **chmod g+w /home** y **chmod g+x /home/**

Con estos comandos lo que hacemos es darle permisos necesarios.

Para acabar la parte de apache, modificamos estos archivos `/etc/apache2/suexec/www-data` y `/etc/apache2/sites-available/000-default.conf`



```
/usr/lib/cgi-bin
/var/www
public_html/cgi-bin
# The first two lines contain the suexec document root and the suexec userdir
# suffix. If one of them is disabled by prepending a # character, suexec will
# refuse the corresponding type of request.
# This config file is only used by the apache2-suexec-custom package. See the
# suexec man page included in the package for more details.
```

```
<VirtualHost *:443>
    ServerName www.gpsystems.es
    ServerAdmin gpsystems@gpsystems

    SuexecUserGroup gyermo gyermo
    <Directory "/usr/lib/cgi-bin/">
        Options +ExecCGI
        AddHandler cgi-script .cgi .pl
        AddHandler default-handler .css .png .jpeg .jpg
    </Directory>
    DocumentRoot /var/www/html
    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # Configuración SSL
    SSLEngine on
    SSLCertificateFile /etc/apache2/certificate/apachecertificate.crt
    SSLCertificateKeyFile /etc/apache2/certificate/apache.key

    # Otras configuraciones específicas para SSL si es necesario
</VirtualHost>
```

Añadimos el SuexecUserGroup para comunicar el usuario que va a ejecutar los scripts cgi.

## 5.Gestion de Usuarios

Se crean dos grupos, profesores y alumnos, para satisfacer la petición del directorio apuntes, creamos este directorio y le asignamos propietario al grupo profesores, y se le dan los permisos necesarios.

```
profesores:x:230:
alumnos:x:231:
root@Gpsystems:~# mkdir /var/www/html/apuntes
root@Gpsystems:~# chown :profesores /var/www/html/apuntes
```

```
root@Gpsystems:~# chmod 755 /var/www/html/apuntes
```

Adicionalmente se crea un enlace simbólico al fichero '/var/log/apache/access.log' para poder visualizar el log de los accesos de los usuarios, sólo podrá ser utilizado por el root

```
ln -s /var/log/apache2/access.log /accesos.log
```

## 6. Directorio skel

Aquí se meten todos los archivos que queremos que tengan todos los usuarios del sistema, como la carpeta apuntes y el archivo condiciones.txt

```
ln -s /var/www/html/apuntes /etc/skel
```

## 7. MariaDB

Como base de datos he elegido MariaDB.

Para instalarla hacemos **apt install mariadb-server mariadbclient**

Después se ejecuta el script **mysql\_secure\_installation** que mejora la seguridad en la instalación mediante el establecimiento de una contraseña (root) para las cuentas root, también permite eliminar las cuentas root que son accesibles desde fuera del local host y eliminar cuentas anónimas.

Posteriormente creamos el usuario, la base de datos y le damos todos los privilegios al usuario sobre la base de datos recién creada, como se ve en la imagen.

```

root@GPSysytems:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 36
Server version: 10.3.39-MariaDB-0+deb10u2 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> CREATE USER 'administrador'@'localhost' IDENTIFIED BY 'admin';
Query OK, 0 rows affected (0,006 sec)

MariaDB [(none)]> create database gpsystems;
Query OK, 1 row affected (0,000 sec)

MariaDB [(none)]> grant all privileges on gpsystems.* to 'administrador'@'localhost';
Query OK, 0 rows affected (0,001 sec)

```

Ahora creo la tabla que va a almacenar cada usuario, con el comando de la imagen.

El state me sirve para ver que las cuentas se han activado correctamente, y tengo un campo para ver si es administrador o no. Los demás campos son los pedidos en el registro.

```

MariaDB [gpsystems]> create table users (id varchar(255) not null primary key, password
-> varchar(255) not null, name varchar(255) not null, surname varchar(255)
-> not null, address varchar(255), phone int(20), state int(20) not null default
-> 1, email varchar(255) not null, local_email varchar(255) not null, is_admin
-> BOOLEAN not null default false, role int(20) not null);
Query OK, 0 rows affected (0,022 sec)

```

Inserto el usuario actual en la base de datos.

```

MariaDB [gpsystems]> INSERT INTO users (id, password, name, surname, state, email, local_email, is_admin, role)
-> VALUES ('nocheweb', 'admin2024', 'administrador', 'gpsystems', 2, 'gpsystems09@gmail.com', 'gpsystems@gpsystems', 1, 2);
Query OK, 1 row affected (0,009 sec)

```

```

MariaDB [gpsystems]> INSERT INTO users (id, password, name, surname, state, email, local_email, is_admin, role) VALUES ('gpsystems', 'admin2024', '
', 2, 'gpsystems09@gmail.com', 'gpsystems@gpsystems', 1, 2);
Query OK, 1 row affected (0,012 sec)

```

```

MariaDB [gpsystems]> select * from users;

```

id	password	name	surname	address	phone	state	email	local_email	is_admin	role
gpsystems	admin2024	administrador	gpsystems	NULL	NULL	2	gpsystems09@gmail.com	gpsystems@gpsystems	1	2

## 8. Quotas

Instalamos con **apt-get install quota**

Deberemos modificar el fichero `/etc/fstab` como se ve en la imagen, añadiendo en `/home` `usrquota` y `grpquota`. Es en `/home` debido a la partición que hice al instalar Debian.

```
GNU nano 3.2 /etc/fstab Modi
# /etc/fstab: static file system information.
#
# Use 'blkid' to print the universally unique identifier for a
# device; this may be used with UUID= as a more robust way to name devices
# that works even if disks are added and removed. See fstab(5).
#
# <file system> <mount point> <type> <options> <dump> <pass>
# / was on /dev/sda1 during installation
UUID=293167ce-887b-4a0c-b779-46f27c5f7a2a / ext4 errors=remount-ro 0 1
# /home was on /dev/sda6 during installation
UUID=e44868dd-ba15-45e3-9574-fabe975aaf0 /home ext4 defaults,usrquota,grpquota 0 2
# swap was on /dev/sda5 during installation
UUID=14234906-e85c-4cba-892c-9be12b9f54fa none swap sw 0 0
/dev/sr0 /media/cdrom0 udf,iso9660 user,noauto 0 0
```

Montamos el sistema de fichero otra vez mediante **`mount -o remount /home`**. Con este comando **`quotacheck -ugmv /home`**, comprobamos que estan bien instaladas.

```
root@GPSystems:~# quotacheck -ugmv /home
quotacheck: Your kernel probably supports journaled quota but you are not using it. Consider switching to journaled quota to avoid running quotacheck after an unclean shutdown.
quotacheck: Scanning /dev/sda6 [/home] done
quotacheck: Cannot stat old user quota file /home/aquota.user: No existe el fichero o el directorio. Usage will not be subtracted.
quotacheck: Cannot stat old group quota file /home/aquota.group: No existe el fichero o el directorio. Usage will not be subtracted.
quotacheck: Cannot stat old user quota file /home/aquota.user: No existe el fichero o el directorio. Usage will not be subtracted.
quotacheck: Cannot stat old group quota file /home/aquota.group: No existe el fichero o el directorio. Usage will not be subtracted.
quotacheck: Checked 158 directories and 3031 files
quotacheck: Old file not found.
quotacheck: Old file not found.
root@GPSystems:~# quotaon -ugv /home
/dev/sda6 [/home]: group quotas turned on
/dev/sda6 [/home]: user quotas turned on
```

Vemos que no están activas y por eso falla, las activamos con **`quotaon -ugv /home`**

## 9.Cron

Primero, configuramos que se borren los usuarios sin confirmar, para ello usamos este comando **`crontab -u root -e`**, y con el editor de texto añadimos la siguiente imagen.

```
# m h dom mon dow command
0 4 * * * /usr/bin/perl /root/borrar_usuario.cgi
```

Para las copias de seguridad instalamos apt install rclone y completamos su configuración. Posteriormente creamos dos directorios, en uno se van a situar las copias de seguridad, mientras que el otro va a ser de respaldo: **`mkdir /nw_back mkdir /nw_back_back`**. En `/nw_back` añadimos los scripts necesarios para la realización de las copias, estos son `'nw_back.sh'` y `'nw_back.pl'`. Y acto seguido usando `crontab -u root -e` añadimos al fichero de tareas periódicas la ejecución del script `'nw_back.sh'` de la siguiente forma:

```
# m h dom mon dow  command
0 4 * * * /usr/bin/perl /root/borrar_usuario.cgi
0 4 * * * /bin/bash /nw_back/nw_back.sh
```

Para la monitorización instalamos acct con **apt install acct**, y lo activamos con **accton**.

Creamos el directorio 'acct' e incluimos los ficheros 'acct.sh' y 'acct.pl'. Añadir al fichero cron la línea para la ejecución del script acct.sh

```
# m h dom mon dow  command
0 4 * * * /usr/bin/perl /root/borrar_usuario.cgi
0 4 * * * /bin/bash /nw_back/nw_back.sh
0 4 * * * /bin/bash /root/acct/acct.sh
```

He decidido instalar monitorix, con **apt install monitorix** , y accediendo a ip:8080/monitorix, comprobamos que funciona correctamente.

Relacionado con la monitorización, tenemos el script avisoroot.pl que nos avisa de que se ha iniciado una sesión. Modificamos '.bashrc' y añadimos perl /root/avisoroot.pl

## 10. Correo

He usado postfix, lo instalamos con **apt install postfix**, eligiendo sitio de internet.

Posteriormente instalamos dovecot **apt install dovecot-imapd** y roundcube **apt install roundcube**.

Para configurarlos, añadimos a '/etc/postfix/main.cf' el tamaño de los mensajes y de los buzones, como se ve en la imagen.

```
GNU nano 3.2 /etc/postfix/main.cf

# fresh installs.
compatibility_level = 2


# TLS parameters
smtpd_tls_cert_file=/etc/ssl/certs/ssl-cert-snakeoil.pem
smtpd_tls_key_file=/etc/ssl/private/ssl-cert-snakeoil.key
smtpd_use_tls=yes
smtpd_tls_session_cache_database = btree:${data_directory}/smtpd_scache
smtp_tls_session_cache_database = btree:${data_directory}/smtp_scache

# See /usr/share/doc/postfix/TLS_README.gz in the postfix-doc package for
# information on enabling SSL in the smtp client.

smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = Gpsystems.home
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
mydestination = $myhostname, Gpsystems, localhost.localdomain, , localhost
relayhost =
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 3145728
message_size_limit = 3145728
recipient_delimiter = +
inet_interfaces = all
inet_protocols = all
```

Modificamos el archivo `/etc/roundcube/config.inc.php` cambiando `default_host` a `localhost` y en el apartado de `smtp user` lo ponemos vacío.

```
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %s - domain name after the '@' from e-mail address provided at login screen
// For example %n = mail.domain.tld, %t = domain.tld
$config['default_host'] = 'localhost';

// SMTP server host (for sending mails).
// Enter hostname with prefix tls:// to use STARTTLS, or use
// prefix ssl:// to use the deprecated SSL over SMTP (aka SMTPS)
// Supported replacement variables:
// %h - user's IMAP hostname
// %n - hostname ($_SERVER['SERVER_NAME'])
// %t - hostname without the first part
// %d - domain (http hostname $_SERVER['HTTP_HOST'] without the first part)
// %z - IMAP domain (IMAP hostname without the first part)
// For example %n = mail.domain.tld, %t = domain.tld
$config['smtp_server'] = 'localhost';

// SMTP port (default is 25; use 587 for STARTTLS or 465 for the
// deprecated SSL over SMTP (aka SMTPS))
$config['smtp_port'] = 25;

// SMTP username (if required) if you use %u as the username Roundcube
// will use the current username for login
$config['smtp_user'] = '';

// SMTP password (if required) if you use %p as the password Roundcube
// will use the current user's password for login
$config['smtp_pass'] = '%p';
```

Por último para que sea accesible desde la web, creamos un enlace simbólico con `ln -s /usr/share/roundcube /var/html/webmail`

## 11. Wordpress

He usado wordpress como sitio personal.

**wget https://wordpress.org/latest.tar.gz**

Lo descomprimos: **tar -zxvf latest.tar.gz**

Cambiamos el propietario y los permisos para que `www-data` pueda acceder sin problemas:  
`chown www-data.www-data /var/www/html/wordpress -R`

Una vez Wordpress está instalado configuramos su base de datos, creamos la base de datos `wpdb`: **CREATE DATABASE wpdb DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4\_unicode\_ci**; Después creamos al usuario `'wpuser'` y le damos permisos sobre la nueva base de datos: **CREATE USER 'wpuser'@'localhost' IDENTIFIED BY 'root'; GRANT ALL PRIVILEGES ON wpdb.\* TO 'wpuser'@'localhost';**

Finalmente entrando a 'direccionIP/wordpress' vemos la interfaz de la web de WordPress y acabamos la instalación de wordpress.

Para permitir a los usuarios del servidor que se registren he añadido la opción de que se pueda registrar cualquier persona, pero con un rol de autor, para que puedan publicar en el sitio. Para hacerlo con una interfaz más amigable, he añadido el plugin theme my login, que permite hacer login y registro en una interfaz más sencilla. Toda la información de esto, la tiene el usuario en el fichero condiciones txt que tiene en su directorio /home, y que también se le envía por correo al activar su cuenta.

A continuación tendrás que introducir los detalles de tu conexión con la base de datos. Si no estás seguro de ellos, contacta con tu proveedor de alojamiento.

**Nombre de la base de datos**

El nombre de la base de datos que quieres usar con WordPress.

**Nombre de usuario**

El nombre de usuario de tu base de datos.

**Contraseña**

Mostrar

  
La contraseña de tu base de datos.

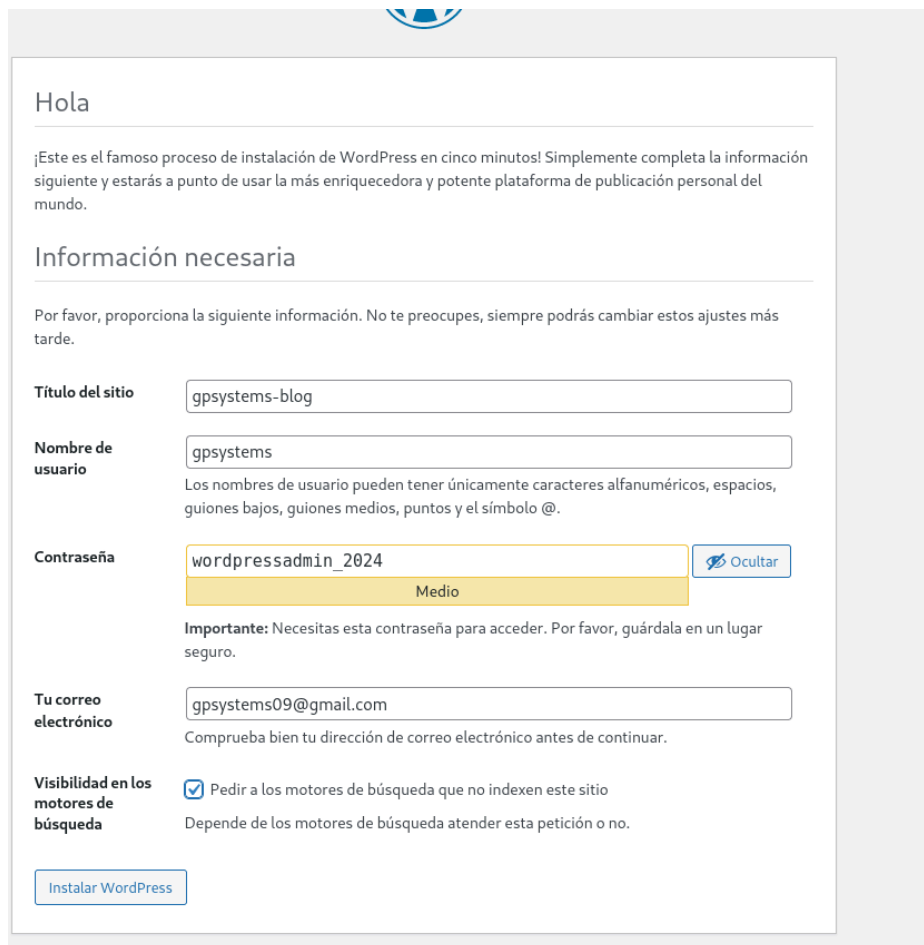
**Servidor de la base de datos**

Si localhost no funciona, deberías poder obtener esta información de tu proveedor de alojamiento web.

**Prefijo de tabla**

Si quieres ejecutar varias instalaciones de WordPress en una sola base de datos cambia esto.

Enviar



Hola

¡Este es el famoso proceso de instalación de WordPress en cinco minutos! Simplemente completa la información siguiente y estarás a punto de usar la más enriquecedora y potente plataforma de publicación personal del mundo.

### Información necesaria

Por favor, proporciona la siguiente información. No te preocupes, siempre podrás cambiar estos ajustes más tarde.

**Título del sitio**

**Nombre de usuario**   
Los nombres de usuario pueden tener únicamente caracteres alfanuméricos, espacios, guiones bajos, guiones medios, puntos y el símbolo @.

**Contraseña**  [Ocultar](#)  
Medio

**Importante:** Necesitas esta contraseña para acceder. Por favor, guárdala en un lugar seguro.

**Tu correo electrónico**   
Comprueba bien tu dirección de correo electrónico antes de continuar.

**Visibilidad en los motores de búsqueda** ☒ Pedir a los motores de búsqueda que no indexen este sitio  
Depende de los motores de búsqueda atender esta petición o no.

[Instalar WordPress](#)

## 12.Moodle

Descargamos moodle desde la página web, posteriormente lo descomprimos, y lo copiamos a /var/www/html

Le cambiamos el propietario y los permisos con **chown www-data.www-data /var/www/html/moodle -R chmod 0755 /var/www/html/moodle -R**

Creamos el directorio '/moodledata' y volvemos a cambiar el propietario y los permisos: **chown www-data /var/www/moodledata -R chmod 0770 /var/www/moodledata -R**

Una vez Moodle está correctamente instalado creamos la base de datos 'moodle':

**CREATE DATABASE moodle DEFAULT CHARACTER SET utf8mb4 COLLATE utf8mb4\_unicode\_ci;**  
Después creamos al usuario 'moodle' y le damos permisos sobre la nueva base de datos:  
**CREATE USER 'moodle'@'localhost' IDENTIFIED WITH IDENTIFIED BY 'root'; GRANT ALL PRIVILEGES ON moodle.\* TO 'moodle'@'localhost'**



Ahora accedemos a ip/moodle y completamos la instalación.

También permitimos que los usuarios se registren, con la opción propia que da moodle para registrarse por correo.

### Confirme las rutas

**Dirección Web**  
Dirección web completa para acceder a Moodle, es decir, la dirección que los usuarios escribirán en la barra de búsqueda del navegador para acceder a Moodle.

No es posible acceder a Moodle utilizando múltiples direcciones. Si su portal tiene varias direcciones debe configurar la más sencilla y configurar un redireccionamiento permanente desde las otras.

Si su portal es accesible desde internet, y desde una red interna (llamada intranet), entonces use la dirección pública aquí.

Si la dirección actual no es correcta, por favor, cambie el URL en la barra de búsqueda de su navegador y reinicie la instalación.

**Directorio de Moodle**  
Ruta completa del directorio que contiene el código de Moodle.

**Directorio de Datos**  
Un directorio en el que Moodle puede guardar los archivos subidos por usuarios.


En este directorio el usuario del servidor web (por lo general 'nobody', 'apache' o 'www-data') debe poder leer y escribir.

No debe poderse acceder a esta carpeta directamente a través de la web.

Si el directorio no existe, el instalador tratará de crearlo.















Dirección Web	<input type="text" value="http://10.0.2.15/moodle"/>
Directorio de Moodle	<input type="text" value="/var/www/html/moodle"/>
Directorio de Datos	<input type="text" value="/var/www/moodldata"/>

[<< Anterior](#) [Siguiente >>](#)



[Expandir todo](#)

## ▼ General

Nombre de usuario		<input type="text" value="admingpsystems"/>
Escoger un método de identificación:		Cuentas manuales
La contraseña debería tener al menos 8 caracter(es), al menos 1 dígito(s), al menos 1 minúscula(s), al menos 1 mayúscula(s), al menos 1 caracter(es) no alfanuméricos como *, -, o #		
Nueva contraseña	 	<input type="password" value="....."/> 
<input type="checkbox"/> Forzar cambio de contraseña 		
Nombre		<input type="text" value="Administrador"/>
Apellido(s)		<input type="text" value="Usuario"/>
Dirección de correo		<input type="text" value="gpsystems09@gmail.com"/>
Visibilidad del correo electrónico		<input type="text" value="Visible para todos"/> 
Ciudad		<input type="text" value="Salamanca"/>
Seleccione su país		<input type="text" value="España"/> 
Zona horaria		<input type="text" value="Zona horaria del servidor (Europa/Berlín)"/> 
Descripción		<input type="text" value="Soy &lt;u&gt;gpsystems&lt;/u&gt;"/>

## 13.Scripts

Se han utilizado las siguientes librerías de cpan. Se instala con **apt install cpanminus**, y luego con **cpanm install nombrelibreria**

### Se han usado estos módulos

- CGI
- CGI::Session
- DBI
- Sudo
- File::Rotate::Backup
- Sys::Hostname
- Socket
- Linux::usermod
- Email::Send::SMTP::Gmail

- File::Copy::Recursive
- MIME::Base64
- Authen::Simple::PAM

Para que todos los scripts se ejecuten correctamente, debemos darle los permisos necesarios, y cambiar el propietario de /usr/lib/cgi-bin, se hace con **chown -R gyermo:gyermo /usr/lib/cgi-bin/**

```
root@gpsystems:/usr/lib/cgi-bin# chmod a+X activacuenta.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X activa_pag.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X cambiar_contraseña.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X cambiar_datos.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X cerrar_sesion.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X desact_pag.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X eliminar.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X login.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X olvidocontra.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X redirect.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X redirect_pag.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X registro.cgi
root@gpsystems:/usr/lib/cgi-bin# chmod a+X servicios.cgi
```

- acct.pl : Crea un archivo que manda las estadísticas al correo del administrador.
- activacuenta.cgi : para activar a los usuarios.
- avisoroot.pl : avisa al administrador de los inicios de sesión.
- cambiar\_datos.cgi : modificar los datos del usuario menos la contraseña.
- cambiar\_contraseña.cgi : modificar la contraseña del usuario.
- cerrar\_sesion.cgi : cierra sesión.
- borrar\_usuario.cgi : eliminar usuarios que no hayan activado la cuenta.
- eliminar.cgi : eliminar de forma permanente a un usuario.
- login.cgi : iniciar sesión.
- nw\_back.pl : realizar copia de seguridad.
- redirect\_pag.cgi y redirect.cgi : controlar la navegación entre la web.
- registro.cgi : permite dar de alta a nuevos usuarios, con la posterior activación.
- olvidocontra.cgi : permite la solicitud de recuerdo de contraseña.
- servicios.cgi : indica a los usuarios el estado de los servicios del sistema.

## 14.Aspectos de seguridad

Para la seguridad de mi servidor he usado rkhunter, para detectar posibles rootkits y demás posibles amenazas para la seguridad de los usuarios.

Lo instalamos con apt install rkhunter.

Posteriormente debemos modificar el archivo /etc/rkhunter.conf, y añadir las siguientes opciones.

Lo primero sería comentar la línea que vemos en la imagen, la de WEB\_CMD=/bin/false

```
GNU nano 3.2 /etc/rkhunter.conf

# Alternatively, the user may specify a completely new command. However, note
# that rkhunter expects the downloaded file to be written to stdout, and that
# everything written to stderr is ignored. For example:
#
#     WEB_CMD="/opt/bin/dlfile --timeout 5m -q"
#
# *BSD users may want to use the 'ftp' command, provided that it supports the
# HTTP protocol:
#
#     WEB_CMD="ftp -o -"
#
# This option has no default value.
#
#WEB_CMD="/bin/false" █
```

Y luego, añadimos un correo para que nos envíe reportes.

```
#
UPDATE_MIRRORS=1

#
# The MIRRORS_MODE option tells rkhunter which mirrors are to be used when
# the '--update' or '--versioncheck' command-line options are given.
# Possible values are:
#     0 - use any mirror
#     1 - only use local mirrors
#     2 - only use remote mirrors
#
# Local and remote mirrors can be defined in the mirrors file by using the
# 'local=' and 'remote=' keywords respectively.
#
# The default value is '0'.
#
MIRRORS_MODE=0

#
# Email a message to this address if a warning is found when the system is
# being checked. Multiple addresses may be specified simply by separating
# them with a space. To disable the option, simply set it to the null string
# or comment it out.
#
# The option may be specified more than once.
#
# The default value is the null string.
#
# Also see the MAIL_CMD option.
#
MAIL_ON_WARNING=gpsystems09@gmail.com
```

Para acabar comprobamos si el archivo de configuración que acabamos de modificar es válido, con rkhunter -C.

Y actualizamos los datos de rkhunter con rkhunter --update. Comprobamos el estado con rkhunter --check.

También he instalado tripwire en el servidor para una mayor seguridad, con **apt install tripwire**. Realizamos la instalación por defecto y ya podremos usarlo, opcionalmente podríamos añadir otras configuraciones para aumentar la seguridad.

## 15.Sftp

Para enjaular los usuarios cuando accedan por sftp, he utilizado el servidor vsftpd, que instalamos con **apt install vsftpd**.

Modificamos el archivo de configuración que se encuentra en `/etc/vsftpd.conf` y reiniciamos el servicio con **`systemctl restart vsftpd.service`**.

También tenemos que crear un enlace simbólico hacia `vsfpd.log`, lo hacemos con **`ln -s /var/log/vsftpd.log /vsftp.log`**

## 16. Html

Se ha diseñado una web bastante simple para que los usuarios puedan acceder y registrarse, como se ven en las siguientes imágenes.

Dispone también de un botón para la ayuda y para recordar la contraseña.



The image shows a web interface for 'Gpsystems'. At the top, the logo 'Gpsystems' is displayed in a light blue font. Below the logo, there are two links: 'Iniciar sesión' (underlined) and 'Regístrate'. The main form consists of two input fields: 'Nombre de usuario' and 'Contraseña', both with a small icon on the left. Below these fields is a large grey button labeled 'Iniciar sesión'. Underneath the button, there are two links: '¿Has olvidado tu contraseña?' and '¿Necesitas ayuda?'.

# Gpsystems

Iniciar sesión

**Registrate**

<input type="text"/>	Nombre de usuario
<input type="text"/>	Correo electrónico
<input type="password"/>	Contraseña
<input type="password"/>	Repite la contraseña
<input type="text"/>	Nombre
<input type="text"/>	Apellidos
<input type="text"/>	Dirección
<input type="text"/>	Teléfono
Elige un rol <span>▼</span>	
<b>Registrate</b>	

[¿Has olvidado tu contraseña?](#)

Una vez, se ha iniciado sesión, se tiene esta web, con todo lo disponible.

Esta sería la vista del administrador.

## BIENVENIDO ESTUDIANTE

<b>Correo</b>	<b>Estado del servidor</b>
<b>Página personal</b>	<b>Configuración</b>
<b>Moodle</b>	<b>Cerrar sesión</b>
<b>Wordpress</b>	

El estado del servidor se veria asi:

## Estado de los Servicios

HTTPS **activo**.

SSH **activo**.

MariaDB **activo**.

SMTP **activo**.

Aquí profesor y estudiante

BIENVENIDO PROFESOR



## BIENVENIDO ESTUDIANTE

<b>Correo</b>	<b>Página personal</b>
<b>Moodle</b>	<b>Configuración</b>
<b>Wordpress</b>	<b>Cerrar sesión</b>
<b>Apuntes</b>	

El estudiante y el profesor pueden ver el directorio apuntes, para ver los archivos subidos a ese directorio

Esta es la página que permite modificar los datos, todo a través de un formulario.

[← Volver](#)

## MODIFICAR DATOS

Introduzca sólo los datos que desea modificar

<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>
<input type="text"/>

**Modificar**

**Eliminar la cuenta**

(Esta acción no se puede deshacer)

## MODIFICAR CONTRASEÑA

<input type="text"/>
<input type="text"/>
<input type="text"/>

**Modificar**



## 17. Bibliografía

<https://metacpan.org/dist/App-cpanminus/view/bin/cpanm>

<https://metacpan.org/pod/Passwd::Unix>

<https://metacpan.org/pod/Sudo>

<https://metacpan.org/dist/PerlPowerTools/view/bin/mkdir>

<https://metacpan.org/pod/Linux::usermod>

<https://metacpan.org/pod/File::Copy::Recursive>

<https://metacpan.org/pod/Module::Rename>

<https://metacpan.org/pod/File::Path>

<https://metacpan.org/pod/CGI::Session>

<https://perldoc.perl.org/Sys::Hostname>

<https://www.monitorix.org/doc-debian.html>

<https://pressroom.hostalia.com/white-papers/configurar-protocolo-ssh/>

<https://openwebinars.net/blog/consejos-seguridad-servidores-apache/L>

[apache-to-run-cgi-scripts-on-an-ubuntu-vps](#)

<https://www.w3docs.com/snippets/html/how-to-redirect-a-web-page-in-html.html>

<https://askubuntu.com/questions/481698/installing-authensimplepam-module-with-cpan-in-ubuntu-fails>

<https://unix.stackexchange.com/questions/157426/what-is-the-regex-to-validate-linux-users>

<https://www.howtoforge.com/tutorial/how-to-install-and-configure-vsftpd/>

<https://docs.vultr.com/how-to-install-rkhunter-on-debian-10>

