



UNIVERSIDAD TECNOLÓGICA DE PANAMÁ
FACULTAD DE INGENIERÍA DE SISTEMAS COMPUTACIONALES
LICENCIATURA EN INGENIERÍA DE SISTEMAS Y
COMPUTACIÓN



SEGURIDAD EN TECNOLOGÍA DE COMPUTACION

Proyecto Final

Metodología para salvaguardar un servidor web

Integrantes:

Cirilo Franco
Eduardo Vásquez
Israel Pérez

Profesor:

José moreno

Cedula:

8-918-469
8-944-948
8-868-626

1IL-152 | 2022

Contenido general

Introducción	4
Marco teórico.....	5
¿Qué es una interfaz de red?.....	5
.....	5
¿Qué es Mod_security?	6
¿Cómo identificar un bloqueo de mod_security?	6
.....	6
.....	7
¿Qué es un ataque XSS o Cross-Site scripting?	8
¿Qué es Mod_evasive?	9
¿Qué son los ataques DoS y DDoS?	9
¿Qué es un ataque de fuerza bruta?.....	11
.....	11
¿Qué es mod_qos?.....	11
¿Qué es un ataque con Slowloris?.....	12
¿Qué es un latch?.....	13
¿Qué es un virtual host?	13
¿Qué es Webmin?	14
Ubuntu Server 20.04	14
¿Qué es un WAF o Web Application Firewall?	15
.....	15
Implementación y desarrollo del servidor	16
Configuración y ajuste de la maquina virtual.....	16
.....	16
Ajuste de los 4 adaptadores de red:.....	16
.....	16
.....	17
.....	17
.....	18
Instalación de Ubuntu server.....	18

.....	19
.....	20
.....	21
.....	21
.....	22
.....	22
.....	23
.....	24
.....	24
.....	25
.....	25
Instalación de webmin	27
.....	28
.....	28
.....	30
.....	30
Configuraciones para administrar mysql desde webmin	31
Desarrollo de host virtual.....	35
.....	35
.....	38
.....	40
qcd.....	40
.....	42
.....	43
Configuración de WordPress	45
.....	46
.....	46
.....	48
Creación de certificado auto firmado ssh.....	49
.....	52
.....	52

.....	55
Instalación de Redis.....	55
.....	55
.....	56
.....	56
.....	57
Mod security	59
Conclusión.....	62
Referencias.....	63

Introducción

Realizaremos un Proyecto de seguridad informática, del mundo real, asegurando los tres pilares de la seguridad la confidencialidad, integridad y disponibilidad de la información protegida. El proyecto se basará en realizar las configuraciones correspondientes a un web server en el cual encontraremos un sitio WEB particionado con arreglos de disco, responde por HTTPS, con un certificado auto firmado, contendrá Mod_Security actúa como firewall de aplicaciones web, el Mod_Evasive el cual protege de ataques a fuerza bruta, Mod_qos para ataques Slowloris entre otras además se instalará wordpress con sus debidos pluggins de seguridad

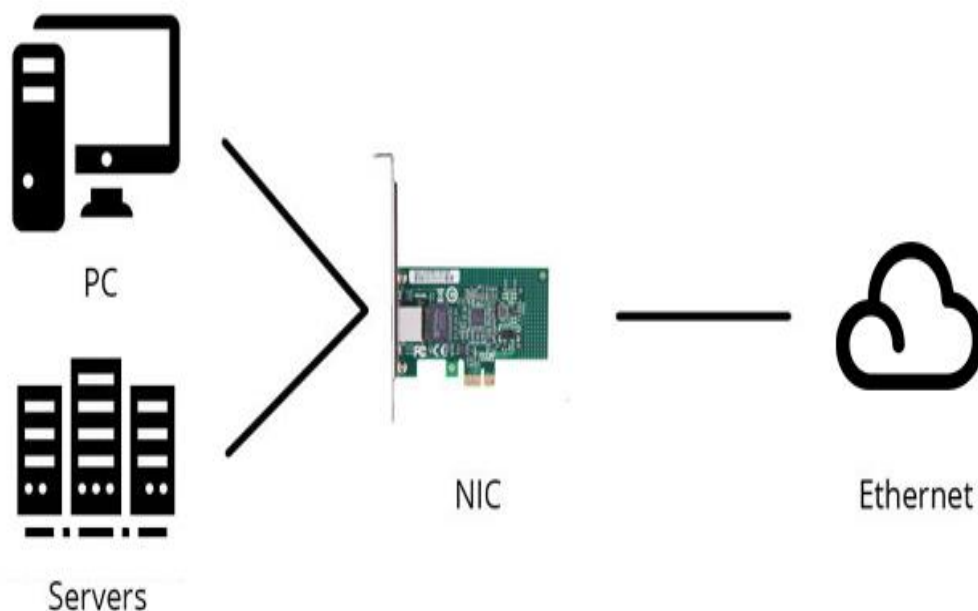
Marco teórico

¿Qué es una interfaz de red?

Es una interfaz que permite o hace posible que servidores que ejecuten un servicio de enrutamiento y acceso remoto para comunicarse con otros equipos por medio de redes privadas o públicas. Las interfaces de red se relacionan con el servidor de enrutamiento y acceso remoto en dos aspectos que ya conocemos, que es tanto en hardware físico, como el adaptador de red y la configuración del software de red (todo sobre redes, s.f.).

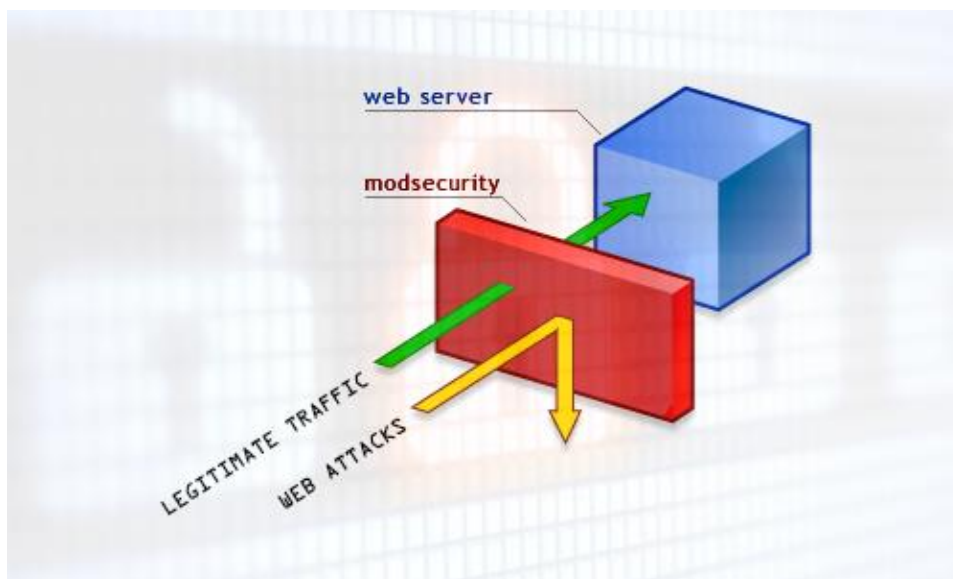
Interfaz privada: Una interfaz privada es un adaptador de red que está físicamente conectado a una red privada. La mayoría de las redes privadas se configuran con un intervalo de direcciones IP de red privada, y la interfaz privada también se configura con una dirección privada.

Interfaz pública: Una interfaz pública es un adaptador de red que está físicamente conectado a una red pública, como Internet. Las interfaces públicas se configuran con una dirección IP pública. Se puede configurar una interfaz pública para que realice la traducción de direcciones de red (NAT).



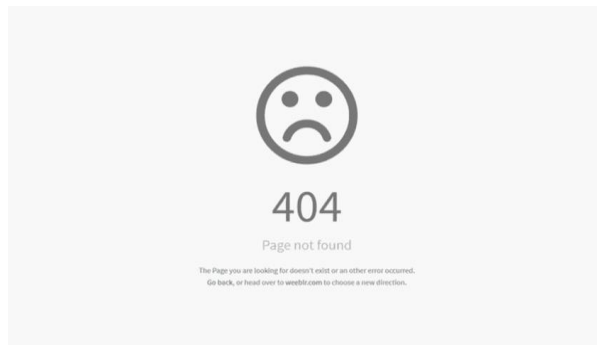
¿Qué es Mod_security?

Mod_security es un modulo de seguridad del servidor web http de código abierto, apache, el cual actura como firewall de aplicaciones web (WAF) y su trabajo es filtrar y bloquear las solicitudes HTTP sospechosas, pudiendo bloquear ataques de fuerza bruta, vulnerabilidades de cross scripting (XSS), ataques por inyección SQL (SQLi), etc. Este modulo esta activo en todos nuestros servidores Linux por defecto. Por lo que no es posible deshabilitar este módulo al 100% por temas de seguridad, este modulo nos permite excepciones mediante ficheros de configuración de alojamientos web para servidores apache conocido como .htacces, en el caso de que trate de un falso positivo (dinahosting, s.f.).



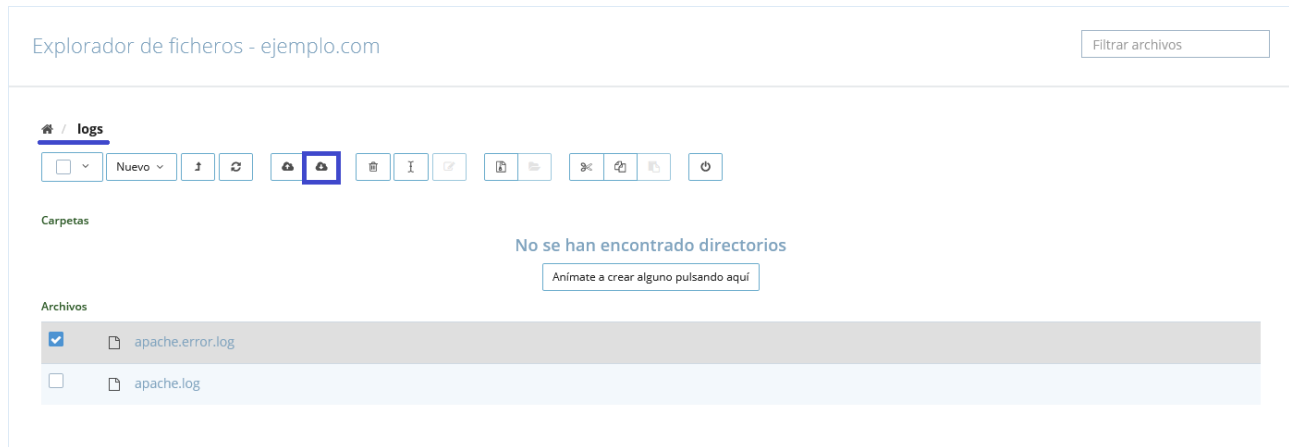
¿Cómo identificar un bloqueo de mod_security?

Si al efectuar alguna tarea en nuestra web, tal como actualizar un formulario, añadir una entrada en WordPress o cualquier otro CMS o realizar un pago a través de un TPV y te encuentras con un error 404, posiblemente estemos ante un bloqueo de mod_security.



Para confirmar que el bloqueo es debido a una regla de mod_security, lo más efectivo sería comprobar el log de errores de Apache disponible en nuestro hosting.

Puedes acceder al log de errores de Apache usando el explorador de ficheros disponible en el apartado FTP de tu hosting, o conectándote mediante FileZilla. El fichero que debes descargar se llama apache.error.log y está ubicado en el directorio logs de tu hosting.



Después de haber descargado el log, abrimos el fichero con cualquier editor de texto y revisamos las ultimas peticiones realizadas, si el log es muy extenso puedes buscar las palabras ModSecurity o simplemente la que contengan tu IP. Cuyas sintaxis serán similares a lo que se muestra a continuación:

```
[Mon Apr 26 13:24:15.571708 2021] [:error] [pid 8xxx:tid 1401138623xxxxx]
[client 123.456.789.012:49500] [client 123.456.789.012] ModSecurity:
Access denied with code 406 (phase 2). Pattern match "^POST$" at
REQUEST_METHOD. [file "/etc/modsecurity/custom/20_bruteforce.conf"] [line
"43"] [id "210"] [msg "Accept header required"] [hostname "ejemplo.com"]
[uri "/"] [unique_id "YIai31JimwwAAB9Mo7EAAA"]
```

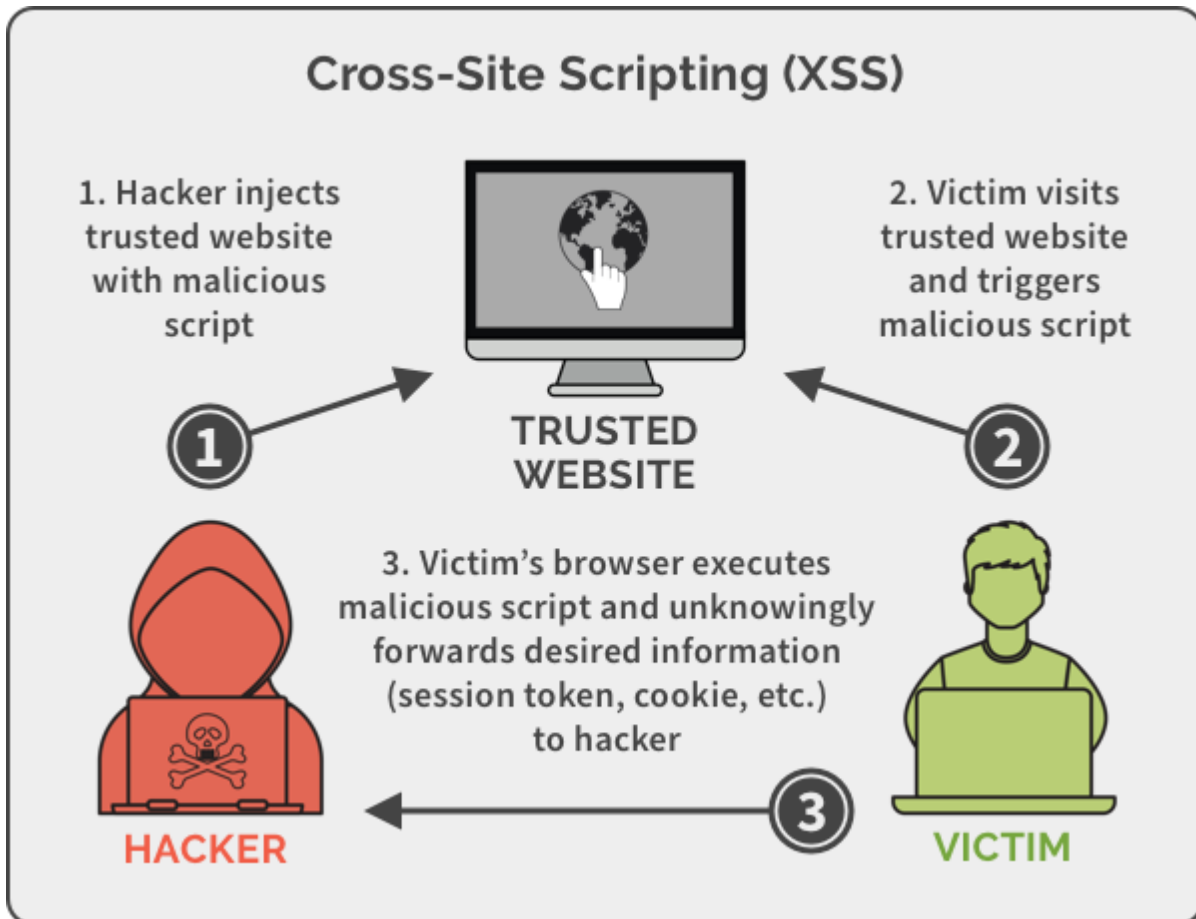
Y la descripción de sus etiquetas son las siguientes:

- **Fecha y hora de la petición:** [Mon Apr 26 13:24:15.571708 2021]
- **IP del visitante:** [client 123.456.789.012]
- **Tipo de error:** ModSecurity: Access denied with code 406 (phase 2)
- **Identificador de error de ModSecurity:** [id "210"]
- **Nuestra web:** [hostname "ejemplo.com"]

¿Qué es un ataque XSS o Cross-Site scripting?

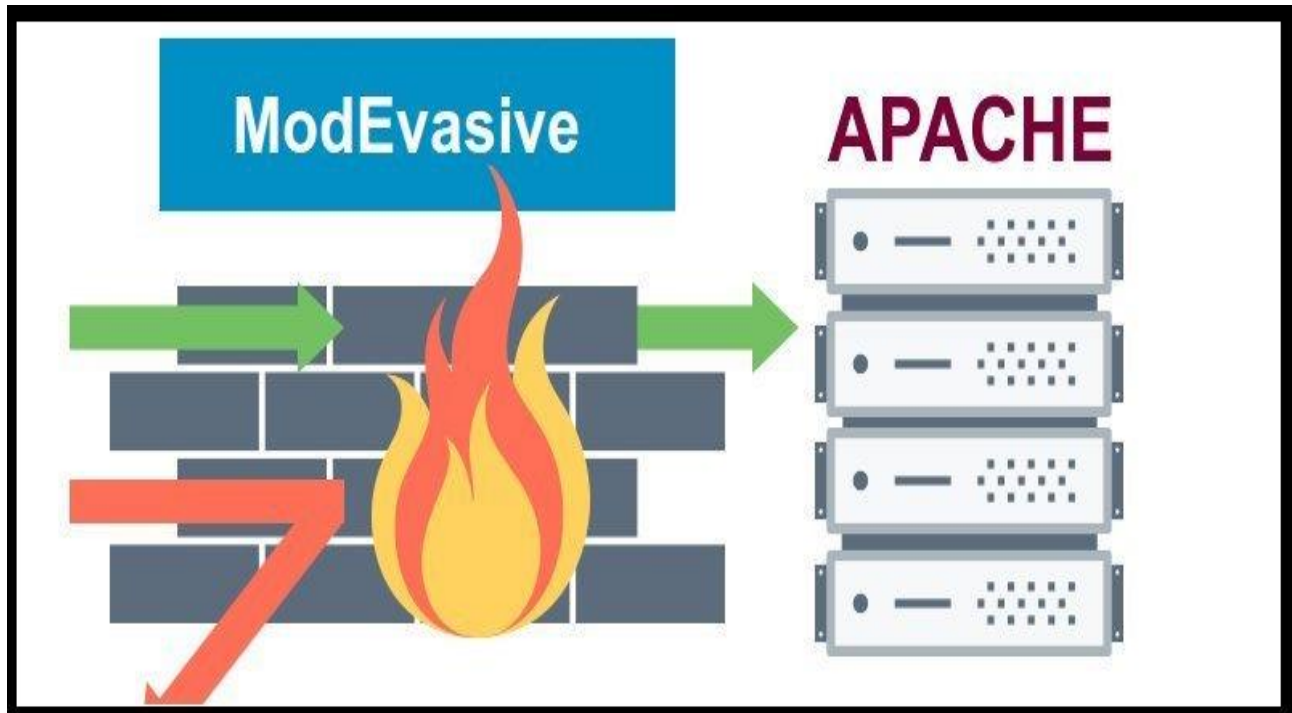
Es un ataque o vulnerabilidad que se aprovecha de falla de seguridad en sitios web y permite a los atacantes implantar scripts maliciosos en un sitio web legítimo para ser ejecutado en el navegador y con objetivos como robo de credenciales, redirigiendo al usuario a otro sitio malicioso, o realizar un cambio de apariencia en paginas web. Básicamente los actores maliciosos inyectan un script malicioso para posteriormente ser procesado (welivesecurity, s.f.). Comúnmente, este proceso que se basa en la confianza que cuenta el sitio sobre la entrada de datos, consiste en enviar un URL con el payload precargado al usuario victima con objetivo determinado o ya definidos como ya antes mencionados tales como:

- Robar datos personales del usuario.
- Cookies de sesión.
- Implementar técnicas de ingeniería social.
- Entre otras.



¿Qué es Mod_evasive?

es un módulo de apache que básicamente lo que hace es mantener una tabla dinámica con las páginas (URIs) accedidas por las distintas direcciones IP de los clientes (navegadores) que acceden al site web (Apache), y permite ejecutar algunas acciones cuando una misma IP (atacante) solicita un mismo recurso (una misma URI o elementos de un mismo sitio) más de n veces en m segundos. (wordpress, 2016)



¿Qué son los ataques DoS y DDoS?

Un ataque de denegación de servicio, tiene como objetivo inhabilitar el uso de un sistema, una aplicación o una máquina, con el fin de bloquear el servicio para el que está destinado. Este ataque puede afectar, tanto a la fuente que ofrece la información como puede ser una aplicación o el canal de transmisión, como a la red informática.

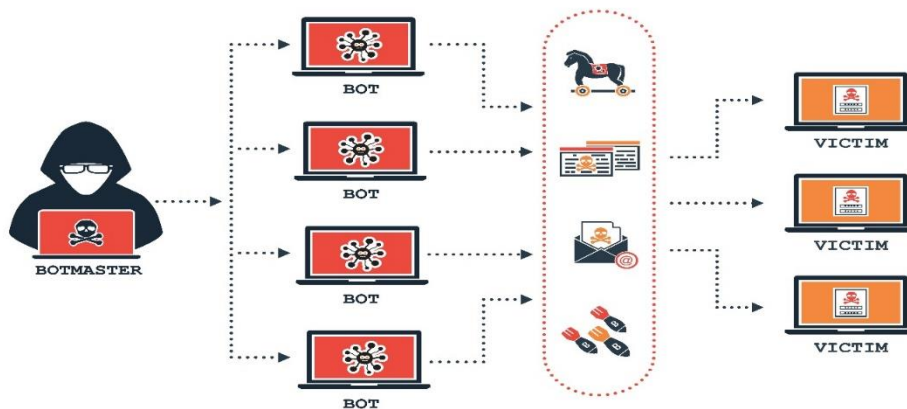
Los servidores web poseen la capacidad de resolver un número determinado de peticiones o conexiones de usuarios de forma simultánea, en caso de superar ese número, el servidor comienza a ralentizarse o incluso puede llegar a no ofrecer respuesta a las peticiones o directamente bloquearse y desconectarse de la red.

Existen dos técnicas de este tipo de ataques: la denegación de servicio o DoS (por sus siglas en inglés Denial of Service) y la denegación de servicio distribuido o DDoS (por sus siglas en inglés Distributed Denial of Service). La diferencia entre ambos es el número de ordenadores o IP's que realizan el ataque.

En los ataques DoS se generan una cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones, esto es cuando se materializa la denegación del servicio.

En el caso de los ataques DDoS, se realizan peticiones o conexiones empleando un gran número de ordenadores o direcciones IP. Estas peticiones se realizan todas al mismo tiempo y hacia el mismo servicio objeto del ataque. Un ataque DDoS es más difícil de detectar, ya que el número de peticiones proviene desde diferentes IP's y el administrador no puede bloquear la IP que está realizando las peticiones, como sí ocurre en el ataque DoS.

Los ordenadores que realizan el ataque DDoS son reclutados mediante la infección de un malware, convirtiéndose así en bots o zombis, capaces de ser controlados de forma remota por un ciberdelincuente. Un conjunto de bots, es decir, de ordenadores infectados por el mismo malware, forman una botnet o también conocida como red zombi. Obviamente, esta red tiene mayor capacidad para derribar servidores que un ataque realizado por sólo una máquina. (osi, 2018)



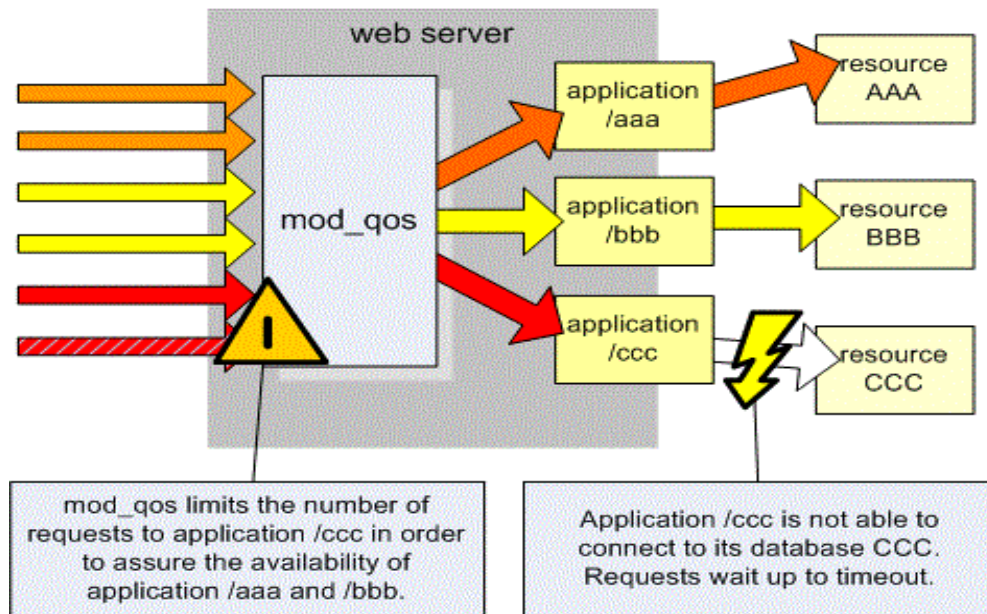
¿Qué es un ataque de fuerza bruta?

Un ataque de fuerza bruta ocurre cuando el atacante emplea determinadas técnicas para probar combinaciones de contraseñas con el objetivo de descubrir las credenciales de una potencial víctima y así lograr acceso a una cuenta o sistema. Existen diferentes tipos de ataque de fuerza bruta, como el “credential stuffing”, el ataque de diccionario, el ataque de fuerza bruta inverso o el ataque de password spraying. Generalmente, los ataques de fuerza bruta tienen mayor éxito en los casos en los que se utilizan contraseñas débiles o relativamente fáciles de predecir. (welivesecurity, 2020)



¿Qué es mod_qos?

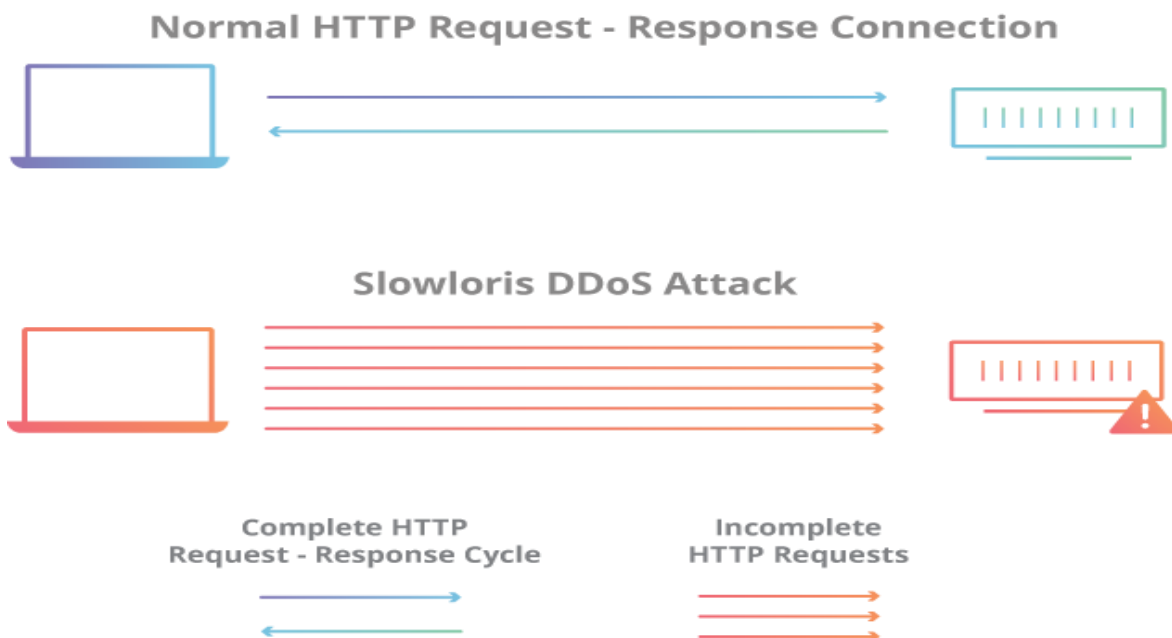
es un módulo de calidad de servicio (QoS) para el servidor Apache HTTP que implementa mecanismos de control que pueden proporcionar diferentes prioridades a diferentes solicitudes. Un servidor web solo puede atender un número limitado de solicitudes simultáneas. QoS se utiliza para garantizar que los recursos importantes permanezcan disponibles bajo una alta carga del servidor. mod_qos se usa para rechazar solicitudes a recursos sin importancia mientras otorga acceso a aplicaciones más importantes. También es posible deshabilitar restricciones de acceso, por ejemplo, para solicitudes a recursos muy importantes o para usuarios muy importantes. (wikipedia, 2021)



¿Qué es un ataque con Slowloris?

Slowloris es un programa de ataque de denegación de servicio que permite que un atacante sobrecargue un servidor objetivo al abrir y mantener muchas conexiones simultáneas HTTP entre el atacante y el objetivo. es un ataque a la capa de aplicación que opera utilizando peticiones HTTP parciales. El ataque funciona al abrir conexiones a un servidor web objetivo y mantener esas conexiones abiertas todo el tiempo que pueda.

Slowloris no es una categoría de ataque, sino que es una herramienta de ataque específica diseñada para permitir que una sola máquina derribe un servidor sin utilizar mucho ancho de banda. A diferencia de los ataques DDoS basados en la reflexión que consumen ancho de banda como amplificación NTP, este tipo de ataque utiliza una baja cantidad de ancho de banda, y en su lugar tiene como objetivo utilizar los recursos del servidor con solicitudes que parecen más lentas de lo normal, pero que por lo demás imitan el tráfico regular. Entra en la categoría de ataques conocidos como ataques "bajos y lentos". (cloudflare, 2022)



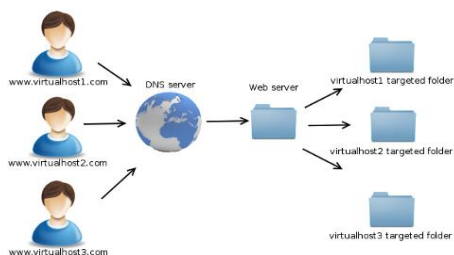
¿Qué es un latch?

es un sistema de pestillos digitales creado por el equipo de elevenpaths que permite abrir y cerrar el acceso a un sitio web cómodamente desde un dispositivo móvil. De esta forma, se puede impedir el acceso a la administración de WordPress mientras no la estemos utilizando. Incluso si alguien conociera nuestros datos de acceso, no podría acceder al sistema mientras Latch esté activado, además de avisarnos de que se ha producido un intento de acceso y tomar así las medidas que consideremos oportunas (TTANDEM, s.f.).

¿Qué es un virtual host?

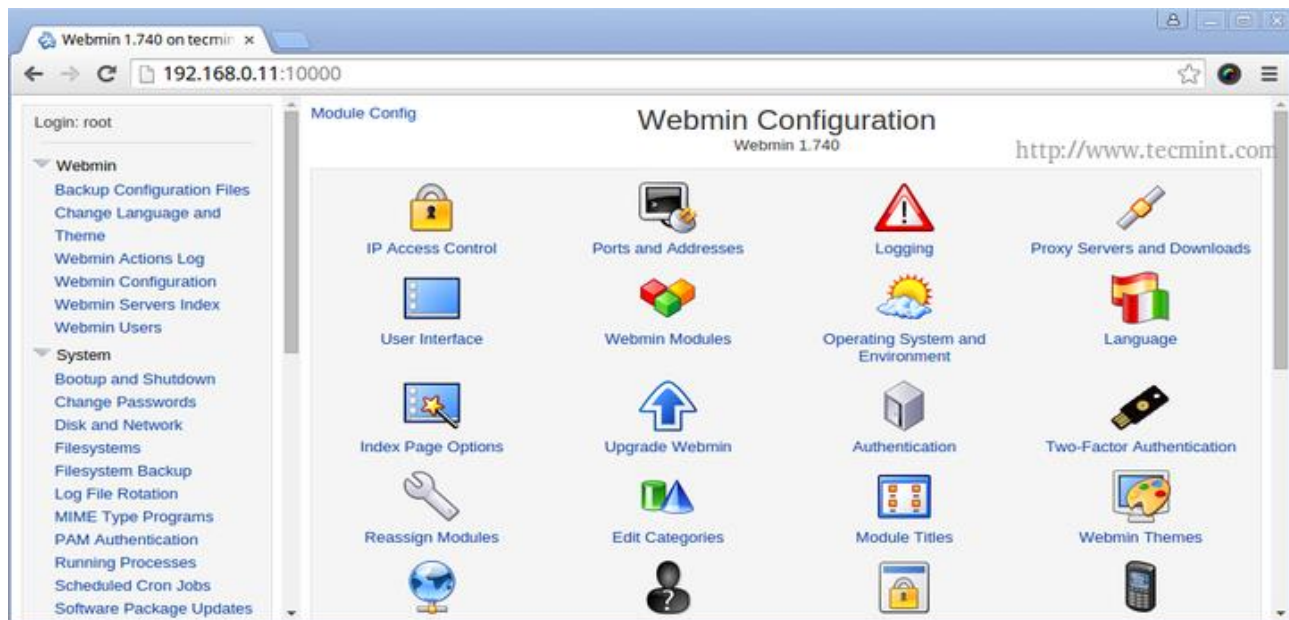
El virtual host, o servidor virtual, es una forma de alojamiento web que permite que varias páginas web puedan funcionar en una misma máquina. Hay dos tipos de virtual host:

Los que se basan en direcciones IP, donde cada página web tendrá una IP diferente. Los que se basan en nombres de dominio, donde una sola dirección IP funcionan varias páginas web. Aunque el navegador tendrá que diferenciar el tipo de virtualhost a la hora de gestionar la petición, la elección de una u otra no tiene ningún efecto para el usuario. (linube, s.f.)



¿Qué es Webmin?

Webmin es una interfaz basada en web para la administración de sistemas para Unix. Usando cualquier navegador web moderno, puede configurar cuentas de usuario, Apache, DNS, compartir archivos y mucho más. Webmin elimina la necesidad de editar manualmente los archivos de configuración de Unix como `/etc/passwd` y le permite administrar un sistema desde la consola o de forma remota. Consulte la página de módulos estándar para obtener una lista de todas las funciones integradas en Webmin.



Ubuntu Server 20.04

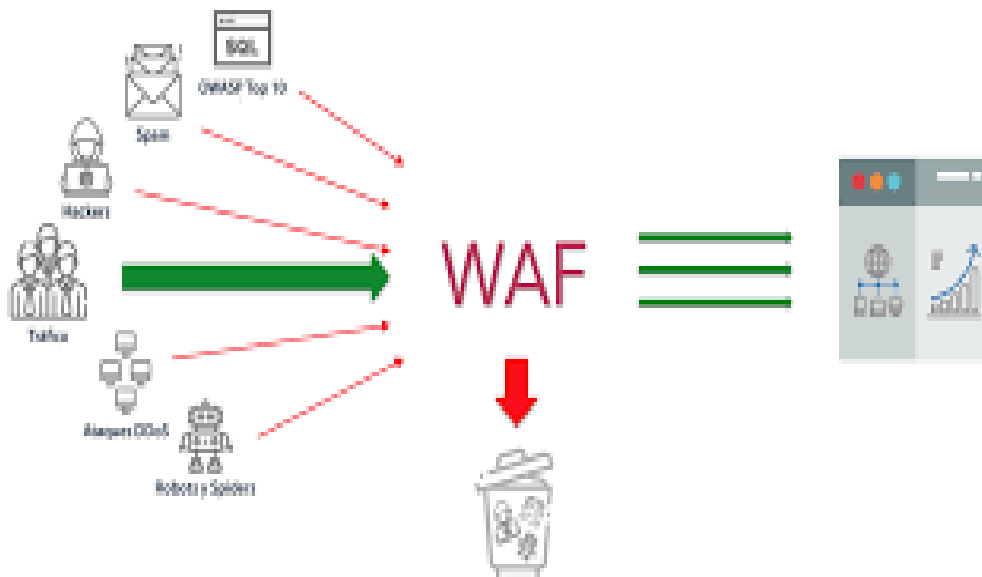
Ubuntu Server es una de las distribuciones Linux más utilizada en servidores Linux, junto con la popular distribución Debian. Este sistema operativo dispone de un gran rendimiento para servidores y funcionalidades de virtualización con Docker entre otras. La última versión LTS de Ubuntu Server es la 20.04 LTS, y tiene soporte completo de actualizaciones de seguridad y mantenimiento hasta el año 2025, además, tenemos soporte adicional de tres años para actualizaciones de seguridad (Redes Zone, s.f.).



¿Qué es un WAF o Web Application Firewall?

No es más que un firewall de aplicación web que ayuda a proteger las aplicaciones web al filtrar y monitorear el tráfico HTTP entre una aplicación web e Internet. Normalmente, protege las aplicaciones web de ataques tales como falsificaciones entre sitios, scripts entre sitios (XSS), inclusiones de archivos e inyecciones de código SQL, entre otros. El WAF es una defensa del protocolo de capa 7 (en el modelo OSI) y no está diseñado para defender de todos los tipos de ataques. Este método de mitigación de ataques suele formar parte de un paquete de herramientas que, en conjunto, crean una defensa integral contra una amplia gama de vectores de ataque.

Al desplegar un WAF en una aplicación web, se coloca un escudo entre la aplicación web e Internet. Si bien un servidor proxy protege la identidad del equipo del cliente por medio de un intermediario, un WAF es un tipo de proxy inverso que protege al servidor de los riesgos al hacer que los clientes atraviesen el WAF antes de llegar al servidor. Este firewall web opera en base de una serie de reglas, comúnmente denominada directivas. Estas directivas tienen como fin proteger contra vulnerabilidades en la aplicación y filtra el tráfico considerado malicioso. El valor de un WAF o firewall de aplicación web consta de la velocidad y sencillez con la que puede aplicar modificaciones en las directivas o reglas que permite una respuesta más rápida ante diversos vectores de ataque.



Implementación y desarrollo del servidor

Configuración y ajuste de la maquina virtual

En este caso ocuparemos virtual box para ejecutar el servidor y configurar de la imagen ISO **Ubuntu server 20.04**.

Para este caso el asignaremos el nombre de servidor web

The screenshot shows the 'Crear máquina virtual' window in VirtualBox. The title bar has a question mark and a close button. Below the title bar is a back arrow and the text 'Crear máquina virtual'. The main heading is 'Nombre y sistema operativo'. Below this is a paragraph: 'Seleccione un nombre descriptivo y una carpeta destino para la nueva máquina virtual y seleccione el tipo de sistema operativo que tiene intención de instalar en ella. El nombre que seleccione será usado por VirtualBox para identificar esta máquina.' There are four input fields: 'Nombre:' with the text 'Servidor Web', 'Carpeta de máquina:' with a folder icon and the path 'C:\Users\jack page\VirtualBox VMs', 'Tipo:' with a dropdown menu showing 'Linux' and a 64-bit icon, and 'Versión:' with a dropdown menu showing 'Oracle (64-bit)'. At the bottom are three buttons: 'Modo experto', 'Next', and 'Cancelar'.

Ajuste de los 4 adaptadores de red:

ajustes de adaptador 1

The screenshot shows the 'Red' (Network) settings for 'Adaptador 1'. The title bar has the word 'Red'. Below the title bar are four tabs: 'Adaptador 1', 'Adaptador 2', 'Adaptador 3', and 'Adaptador 4'. Below the tabs is a checkbox labeled 'Habilitar adaptador de red' which is checked. Below the checkbox is a label 'Conectado a:' followed by a dropdown menu showing 'NAT'. Below the dropdown menu is a label 'Nombre:' followed by a text input field. At the bottom is a blue play button icon followed by the text 'Avanzadas'.

Ajustes de adaptador 2

Red

Adaptador 1

Adaptador 2

Adaptador 3

Adaptador 4

☒ Habilitar adaptador de red

Conectado a:

Adaptador puente

Nombre:

Intel(R) Wi-Fi 6 AX201 160MHz

[▶ Avanzadas](#)

Ajustes de adaptador 3

Red

Adaptador 1

Adaptador 2

Adaptador 3

Adaptador 4

☒ Habilitar adaptador de red

Conectado a:

Adaptador sólo-anfitrión

Nombre:

VirtualBox Host-Only Ethernet Adapter #2

[▶ Avanzadas](#)

Ajustes de adaptador 4

Red

Adaptador 1 Adaptador 2 Adaptador 3 **Adaptador 4**

☒ Habilitar adaptador de red

Conectado a: Red NAT

Nombre: NatNetwork

▶ Avanzadas

Instalación de Ubuntu server

Instalación de la ISO Ubuntu server en la máquina virtual, una vez instalado procedemos a iniciar y configurar nuestra ISO.

Almacenamiento

Dispositivos de almacenamiento

- Controlador: IDE
 - ubuntu-22.04-live-server-amd64.iso
- Controlador: SATA
 - Servidor Web.vdi

Atributos

Unidad óptica: IDE primario maestro

☐ CD/DVD vivo

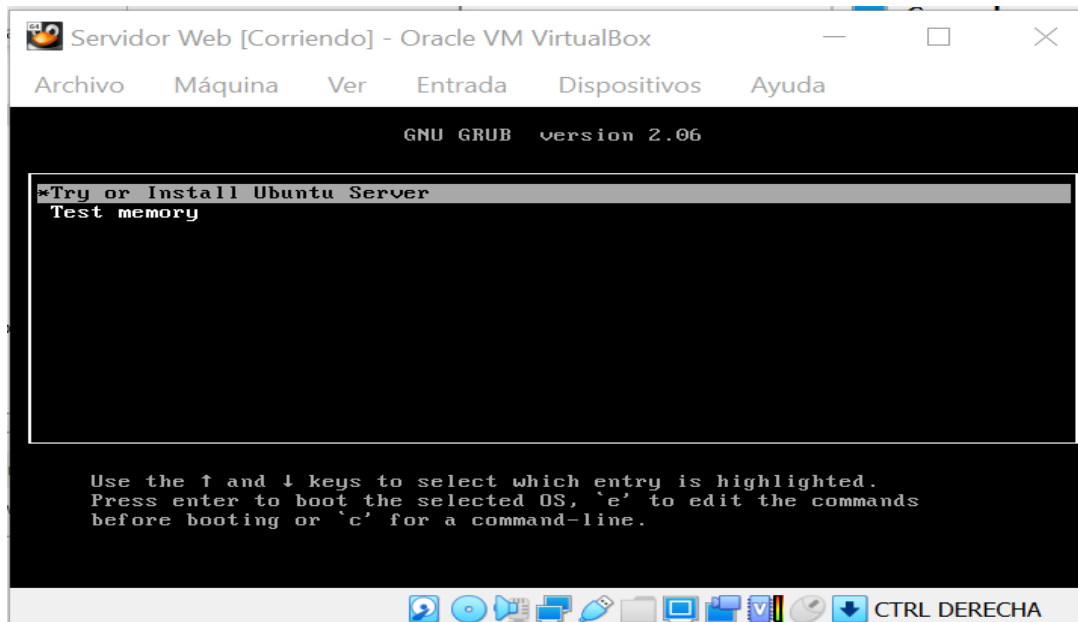
Información

Tipo: Imagen

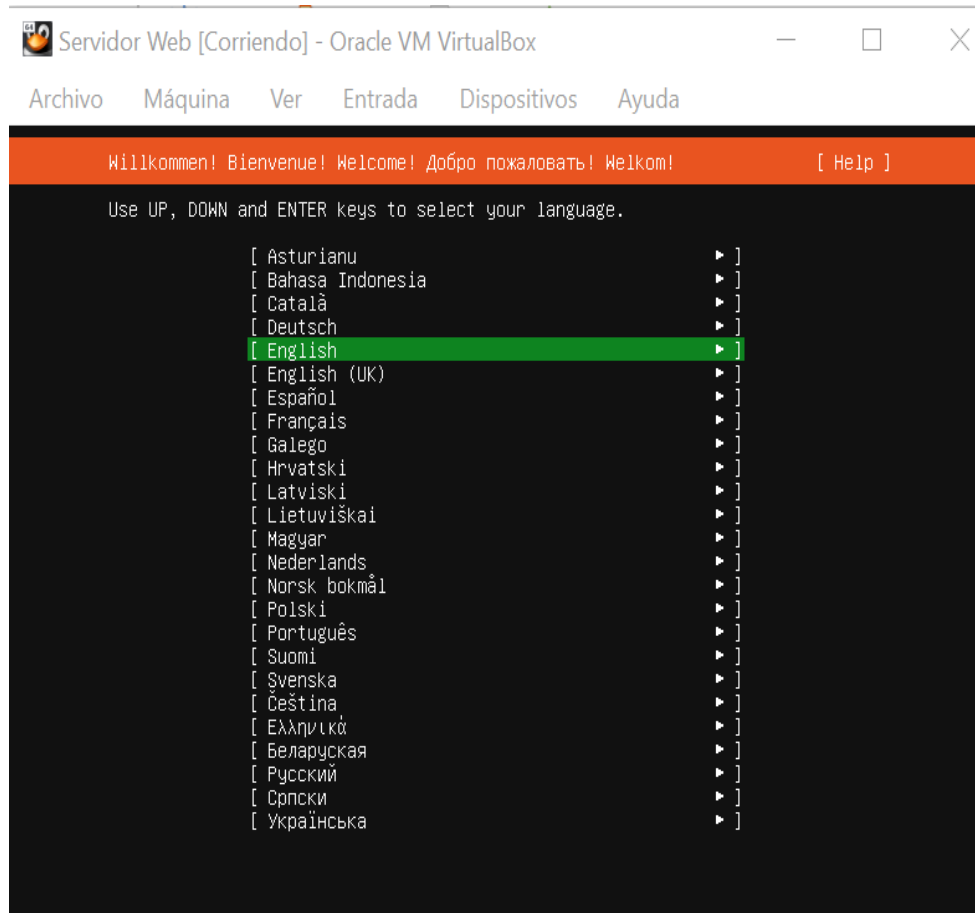
Tamaño: 1.37 GB

Ubicación: C:\Users\jack page\Desktop\DELL\

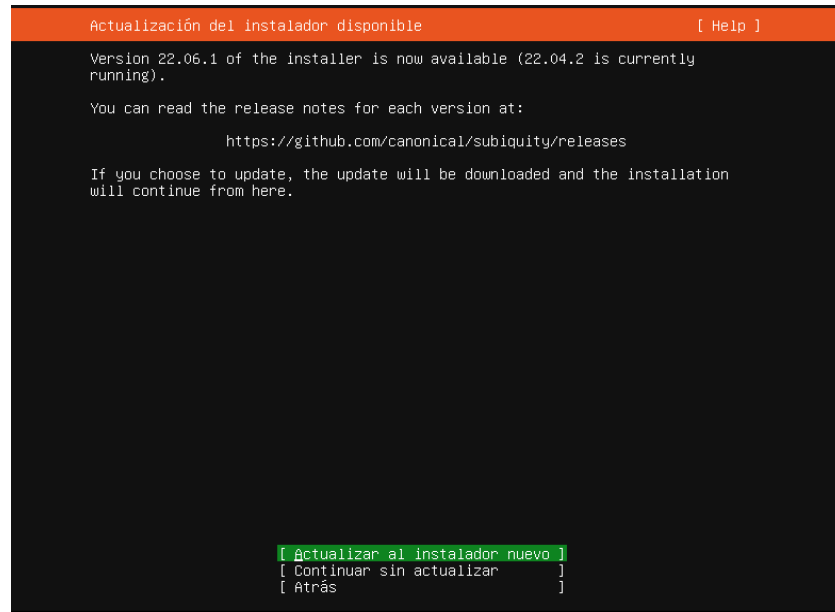
Seleccionamos en instalar Ubuntu server



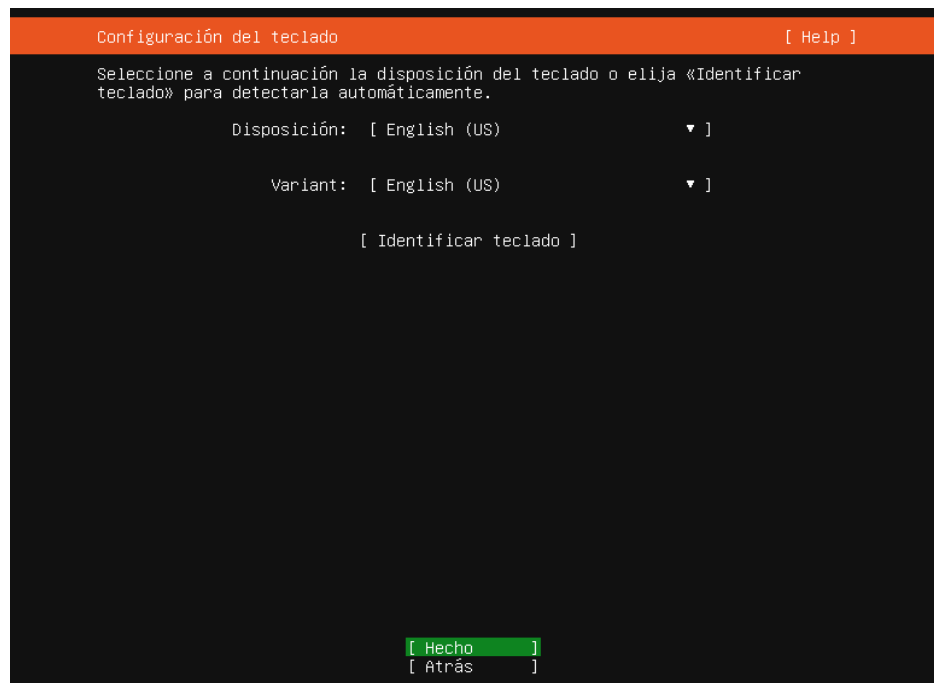
Seleccionamos el idioma



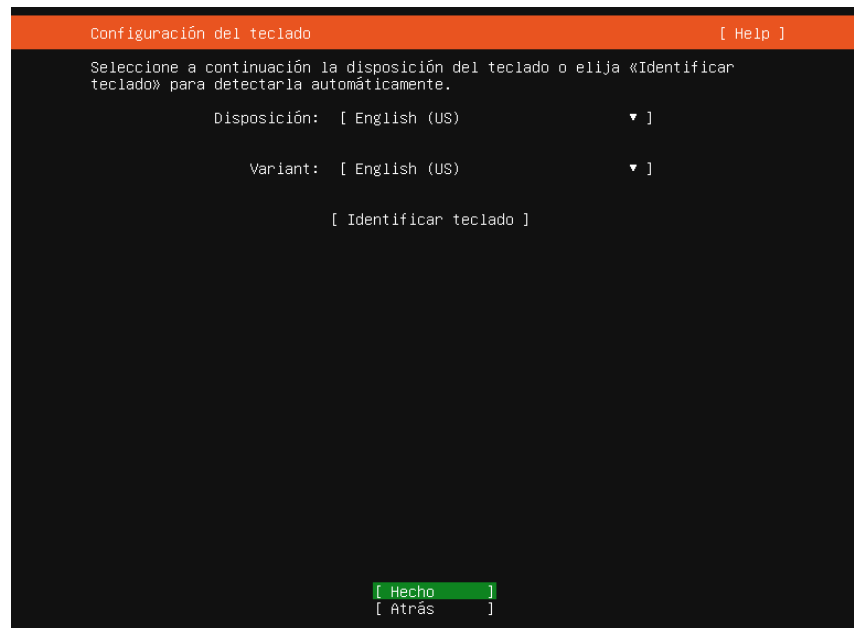
seleccionamos la opción actualizar al instalador nuevo



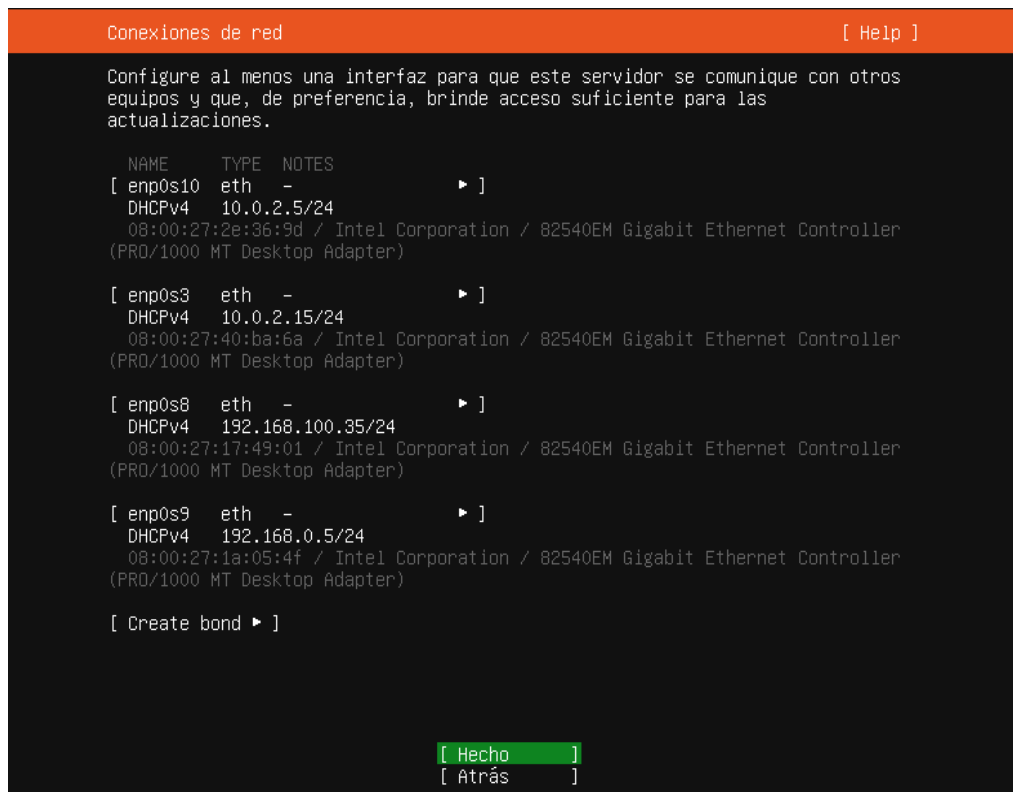
Este es la configuración del teclado el cual lo podemos dejar como esta para que detecte el idioma de nuestro teclado, seleccionamos hecho.



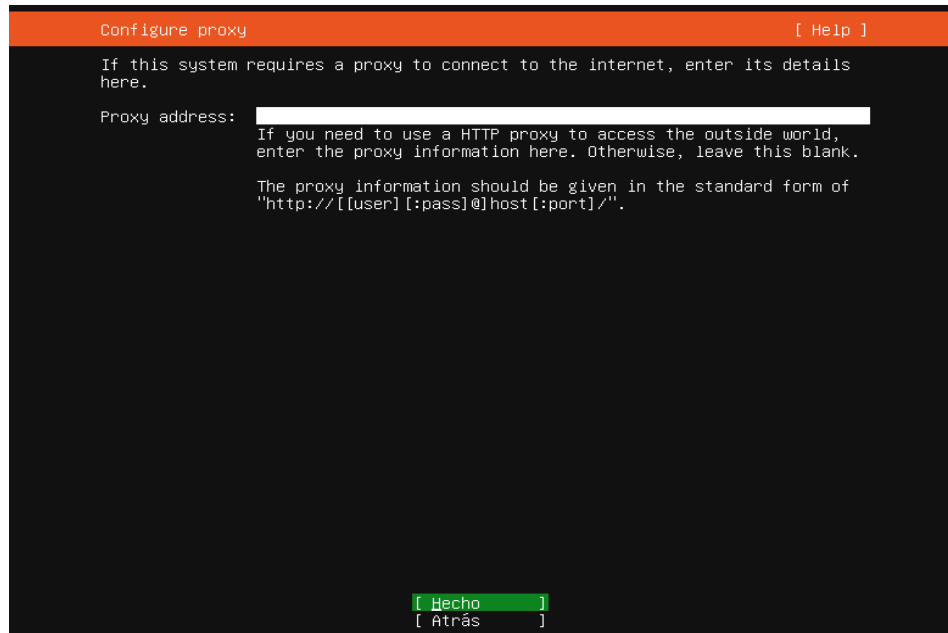
Seleccionamos Ubuntu server, ya que este es la versión predeterminada y seleccionamos hecho.



Posteriormente nos aparecerá los ajustes de interface de red, este se puede dejar en el ajuste que viene por defecto y oprimimos en hecho.



Nos consulta si nuestro sistema requiere de un proxy y que ingresemos los detalle, por lo que no ingresaremos nada ya que no daremos uso de proxy y oprimimos hecho.



Configure proxy [Help]

If this system requires a proxy to connect to the internet, enter its details here.

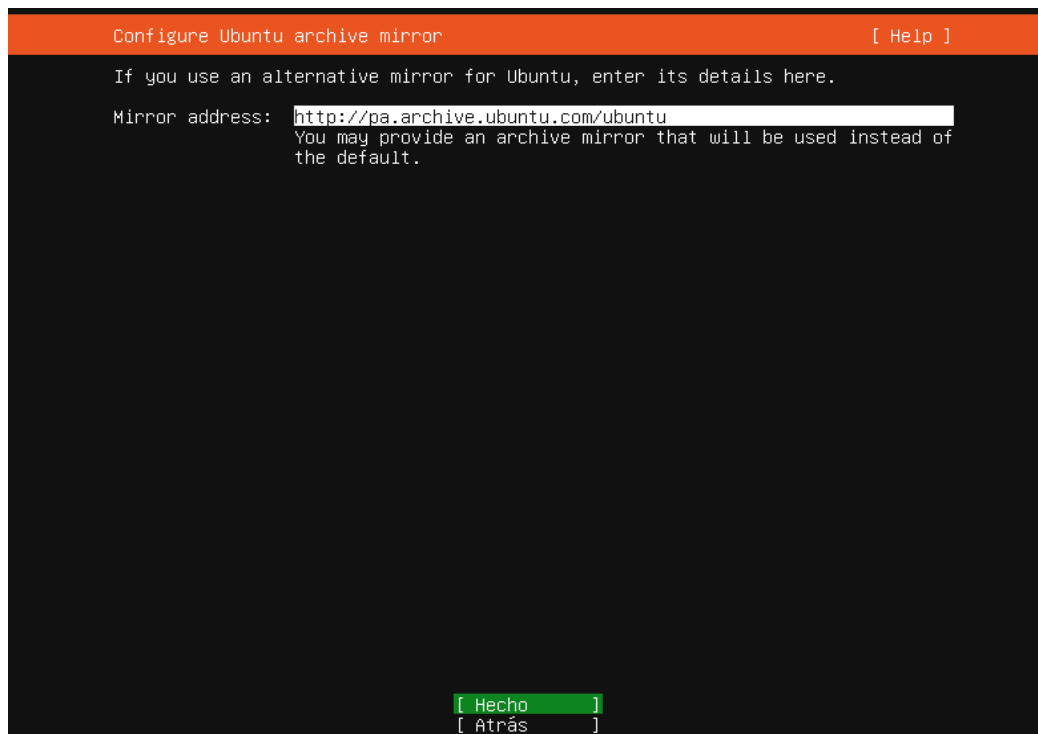
Proxy address:

If you need to use a HTTP proxy to access the outside world, enter the proxy information here. Otherwise, leave this blank.

The proxy information should be given in the standard form of "http://[[user] [:pass]@]host[:port]/".

[Hecho]
[Atrás]

Nos consulta si contamos con una característica distribución de actualizaciones o espejo de Ubuntu por lo que lo dejamos como tal y oprimimos en hecho.



Configure Ubuntu archive mirror [Help]

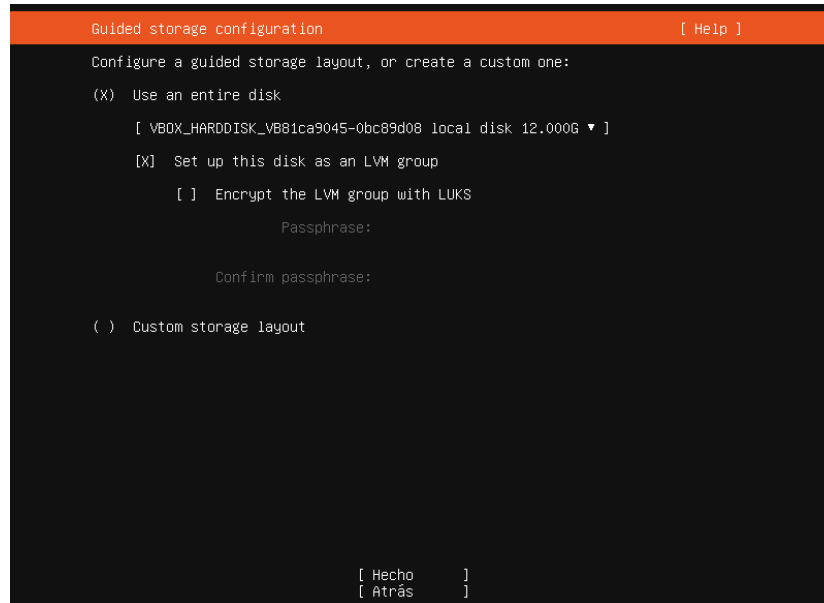
If you use an alternative mirror for Ubuntu, enter its details here.

Mirror address:

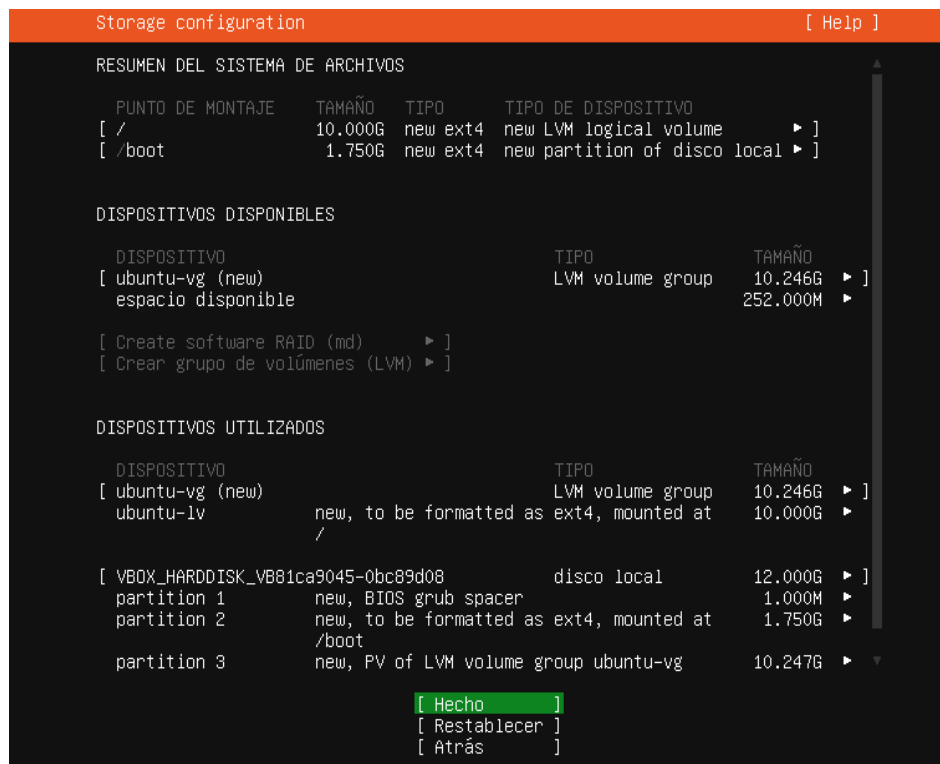
You may provide an archive mirror that will be used instead of the default.

[Hecho]
[Atrás]

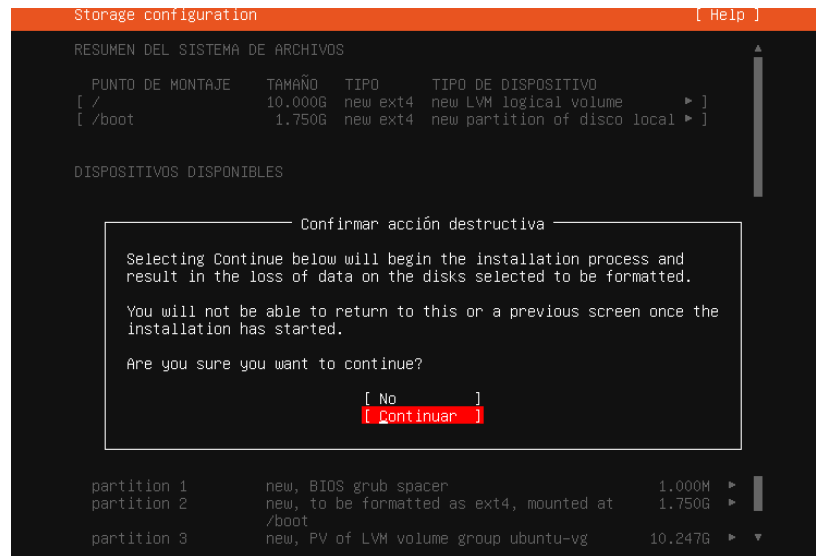
Luego nos preguntara si deseamos configurar un diseño de almacenamiento guiado o crear uno personalizado, el cual procedemos a dejar por defecto y oprimimos hecho.



Luego nos muestra los ajustes que contamos en nuestro sistema de archivos y luego oprimimos en hecho.



nos aparecerá un mensaje el cual nos dice que formateara el disco seleccionado y comenzara la instalación, el cual le daremos continuar.



Nos aparecerá un formulario para ingresar nuestros datos el cual llenaremos de la siguiente manera y luego oprimimos en hecho.

The screenshot shows the 'Configuración de perfil' window with a title bar containing '[Help]'. The main content is a form for user and system configuration. It includes a text box for 'Su nombre:' with the value 'jack', a text box for 'El nombre del servidor:' with the value 'servidocei', a text box for 'Elija un nombre de usuario:' with the value 'usercei', a text box for 'Elija una contraseña:' with the value '*****', and a text box for 'Confirme la contraseña:' with the value '*****'. At the bottom, there is a button labeled '[Hecho]'.

Configuración de perfil [Help]

Proporcione el nombre de usuario y la contraseña que utilizará para acceder al sistema. Puede configurar el acceso SSH en la pantalla siguiente, pero aun se necesita una contraseña para sudo.

Su nombre: jack

El nombre del servidor: servidocei
El nombre que utiliza al comunicarse con otros equipos.

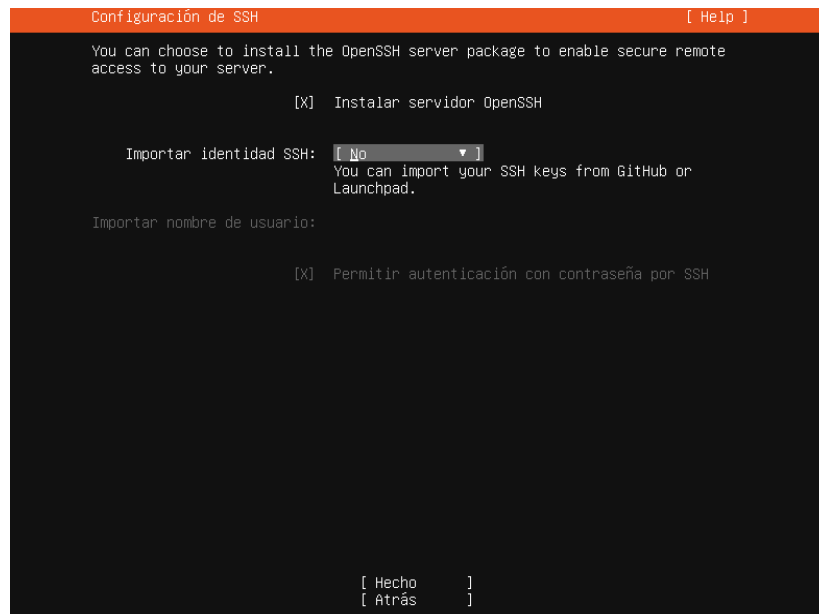
Elija un nombre de usuario: usercei

Elija una contraseña: *****

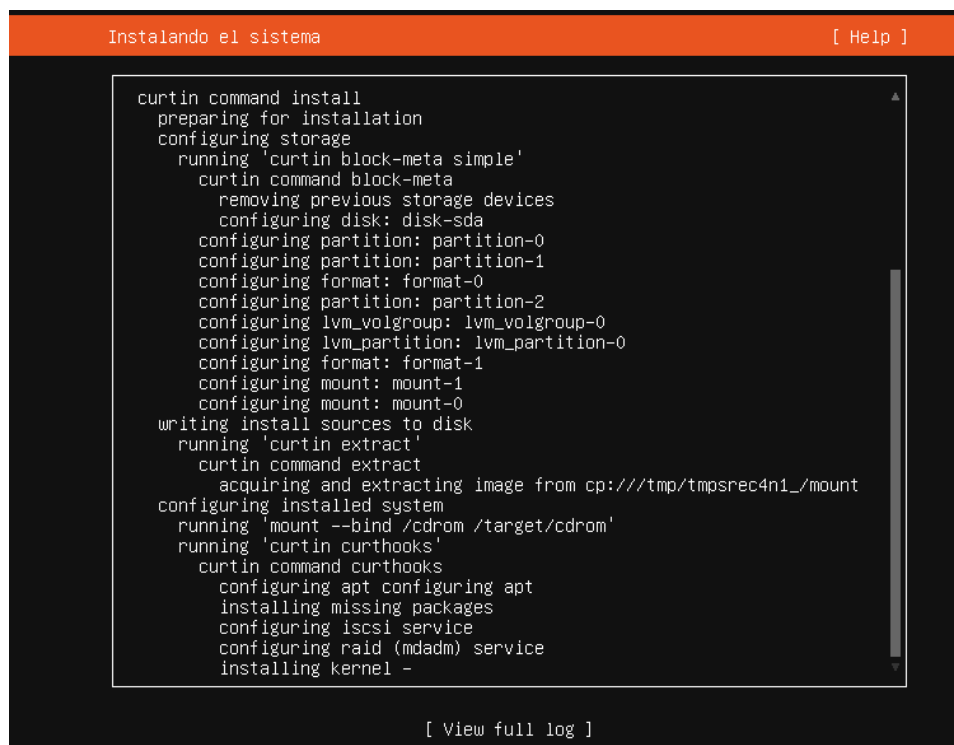
Confirme la contraseña: *****

[Hecho]

Luego nos consulta si deseamos instalar el paquete del servidor open ssh para habilitar el acceso remoto seguro al servidor el cual lo elegimos y en la otra opción escogemos **No** y oprimimos en hecho.



Luego nos indica una serie de instantáneas o copias del disco del sistema el cual podemos elegir, por lo que lo dejaremos por defecto y oprimimos en hecho, para posteriormente comenzar la instalación.



Si la instalación se realizó perfectamente nos debe salir una ventana como esta el cual debemos colocar iniciar sesión con el nombre de usuario y contraseña ingresados anteriormente.

```
Ubuntu 22.04 LTS sevidocei tty1
sevidocei login:
sevidocei login:
sevidocei login:
sevidocei login:
```

Una vez iniciado sesión nos aparecerá una terminal con las respectivas configuraciones de red y el sistema de texto listo para recibir comandos, en caso de que no se nos aparezca la interface de red con el comando **ifconfig**, ingresamos el comando `sudo apt install net-tools` para instalar las herramientas de red.

```
* Documentation:  https://help.ubuntu.com
* Management:    https://landscape.canonical.com
* Support:        https://ubuntu.com/advantage

System information as of jue 14 jul 2022 05:14:03 UTC

System load:  0.00244140625   Users logged in:      0
Usage of /:   45.2% of 9.75GB IPv4 address for enp0s10: 10.0.2.7
Memory usage: 21%           IPv4 address for enp0s3:  10.0.2.15
Swap usage:   0%            IPv4 address for enp0s8:  192.168.100.35
Processes:   106            IPv4 address for enp0s9:  192.168.0.7

24 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

usercei@sevidocei:~$ _
```

Instalación de webmin

A continuación, instalaremos un sistema de administración de sitios web para la configuración de cuentas de usuario, apache, DNS, de nuestro servidor.

Ejecutamos el comando: **sudo vi /etc/apt/sources.list**, y se nos desplegara una ventana que se nos muestra a continuación, en donde se nos muestra los paquetes a instalar, suendo este el archivo fuente de repositorios.

```
% See http://help.ubuntu.com/community/UpgradeNotes for how to upgrade to
# newer versions of the distribution.
deb http://pa.archive.ubuntu.com/ubuntu jammy main restricted
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy main restricted

## Major bug fix updates produced after the final release of the
## distribution.
deb http://pa.archive.ubuntu.com/ubuntu jammy-updates main restricted
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy universe
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy universe
deb http://pa.archive.ubuntu.com/ubuntu jammy-updates universe
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy multiverse
deb http://pa.archive.ubuntu.com/ubuntu jammy-updates multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-updates multiverse

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy-backports main restricted universe multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-backports main restricted universe multiverse

"/etc/apt/sources.list" 42L, 2437B                               1,1      Comienzo
```

Bajamos un poco de la ventana e ingresamos la siguiente dirección:

deb http://download.webmin.com/download/repository sarge contrib

```
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
deb http://pa.archive.ubuntu.com/ubuntu jammy-updates main restricted
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-updates main restricted

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team. Also, please note that software in universe WILL NOT receive any
## review or updates from the Ubuntu security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy universe
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy universe
deb http://pa.archive.ubuntu.com/ubuntu jammy-updates universe
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-updates universe

## N.B. software from this repository is ENTIRELY UNSUPPORTED by the Ubuntu
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy multiverse
deb http://pa.archive.ubuntu.com/ubuntu jammy-updates multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-updates multiverse

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy-backports main restricted universe multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-backports main restricted universe multiverse

deb http://pa.archive.ubuntu.com/ubuntu jammy-security main restricted
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-security main restricted
deb http://pa.archive.ubuntu.com/ubuntu jammy-security universe
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-security universe
deb http://pa.archive.ubuntu.com/ubuntu jammy-security multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-security multiverse
deb http://download.webmin.com/download/repository sarge contrib_
INSERTAR 43,65 Final
```

Una vez hecho esto mantenemos oprimido la tecla esc y escribimos dos puntos y wq para guardar y salir del archivo.

```
## team, and may not be under a free licence. Please satisfy yourself as to
## your rights to use the software. Also, please note that software in
## multiverse WILL NOT receive any review or updates from the Ubuntu
## security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy multiverse
deb http://pa.archive.ubuntu.com/ubuntu jammy-updates multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-updates multiverse

## N.B. software from this repository may not have been tested as
## extensively as that contained in the main release, although it includes
## newer versions of some applications which may provide useful features.
## Also, please note that software in backports WILL NOT receive any review
## or updates from the Ubuntu security team.
deb http://pa.archive.ubuntu.com/ubuntu jammy-backports main restricted universe multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-backports main restricted universe multiverse

deb http://pa.archive.ubuntu.com/ubuntu jammy-security main restricted
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-security main restricted
deb http://pa.archive.ubuntu.com/ubuntu jammy-security universe
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-security universe
deb http://pa.archive.ubuntu.com/ubuntu jammy-security multiverse
# deb-src http://pa.archive.ubuntu.com/ubuntu jammy-security multiverse
deb http://download.webmin.com/download/repository sarge contrib

"/etc/apt/sources.list" 54L, 2512B escritos
usercel@sevidocel:~$
```

Una vez guardado los respectivos cambios en el archivo procedemos a ejecutar el siguiente comando:

wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -, luego

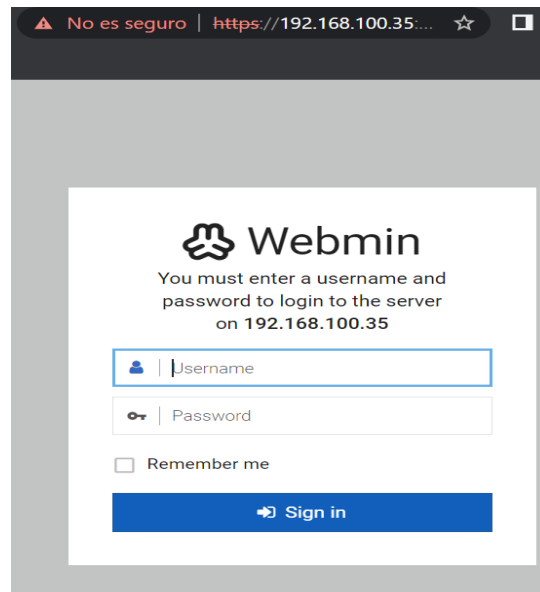
actualizamos el repositorio con el comando **sudo apt-get update**.

```
"/etc/apt/sources.list" 54L, 2512B escritos
usercei@sevidocei:~$ wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
usercei@sevidocei:~$ wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
usercei@sevidocei:~$ sudo apt-get update
Ign:1 http://download.webmin.com/download/repository sarge InRelease
Obj:2 http://pa.archive.ubuntu.com/ubuntu jammy InRelease
Des:3 http://pa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Des:4 http://download.webmin.com/download/repository sarge Release [16,9 kB]
Des:5 http://download.webmin.com/download/repository sarge Release.gpg [173 B]
Des:6 http://download.webmin.com/download/repository sarge/contrib amd64 Packages [1.378 B]
Des:7 http://pa.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Des:8 http://pa.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:9 http://pa.archive.ubuntu.com/ubuntu jammy/main Translation-es [332 kB]
Des:10 http://pa.archive.ubuntu.com/ubuntu jammy/restricted Translation-es [964 B]
Des:11 http://pa.archive.ubuntu.com/ubuntu jammy/universe Translation-es [1.356 kB]
Des:12 http://pa.archive.ubuntu.com/ubuntu jammy/multiverse Translation-es [68,2 kB]
Descargados 2.101 kB en 7s (317 kB/s)
Reading package lists... Done
W: http://download.webmin.com/download/repository/dists/sarge/Release.gpg: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
usercei@sevidocei:~$
```

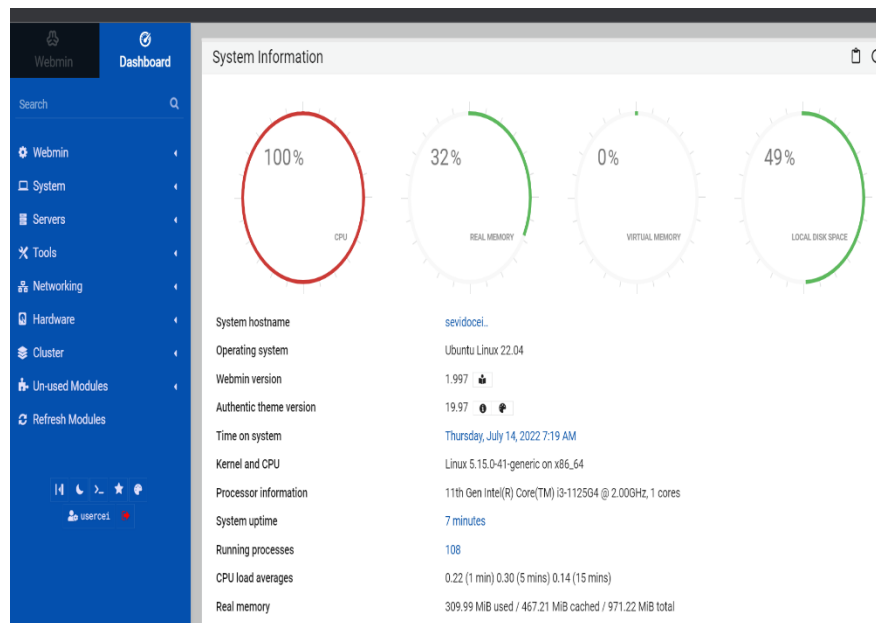
Instalamos el webmin con **sudo apt-get install webmin** e ingresamos **S** y oprimimos enter para continuar.

```
usercei@sevidocei:~$ wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
usercei@sevidocei:~$ wget -q http://www.webmin.com/jcameron-key.asc -O- | sudo apt-key add -
Warning: apt-key is deprecated. Manage keyring files in trusted.gpg.d instead (see apt-key(8)).
OK
usercei@sevidocei:~$ sudo apt-get update
Ign:1 http://download.webmin.com/download/repository sarge InRelease
Obj:2 http://pa.archive.ubuntu.com/ubuntu jammy InRelease
Des:3 http://pa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Des:4 http://download.webmin.com/download/repository sarge Release [16,9 kB]
Des:5 http://download.webmin.com/download/repository sarge Release.gpg [173 B]
Des:6 http://download.webmin.com/download/repository sarge/contrib amd64 Packages [1.378 B]
Des:7 http://pa.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Des:8 http://pa.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:9 http://pa.archive.ubuntu.com/ubuntu jammy/main Translation-es [332 kB]
Des:10 http://pa.archive.ubuntu.com/ubuntu jammy/restricted Translation-es [964 B]
Des:11 http://pa.archive.ubuntu.com/ubuntu jammy/universe Translation-es [1.356 kB]
Des:12 http://pa.archive.ubuntu.com/ubuntu jammy/multiverse Translation-es [68,2 kB]
Descargados 2.101 kB en 7s (317 kB/s)
Reading package lists... Done
W: http://download.webmin.com/download/repository/dists/sarge/Release.gpg: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
usercei@sevidocei:~$ sudo apt-get install webmin
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Se instalarán los siguientes paquetes adicionales:
  libauthen-pam-perl libio-pty-perl libnet-ssleay-perl perl-openssl-defaults unzip
Paquetes sugeridos:
  zip
Se instalarán los siguientes paquetes NUEVOS:
  libauthen-pam-perl libio-pty-perl libnet-ssleay-perl perl-openssl-defaults unzip webmin
0 actualizados, 6 nuevos se instalarán, 0 para eliminar y 24 no actualizados.
Se necesita descargar 28,9 MB de archivos.
Se utilizarán 305 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```

Una vez instalado accedemos al webmin con nuestra ip de la siguiente manera:
`https://192.168.100.35:10000` y luego iniciamos sesión, por lo que es recomendable cambiar de nombre de usuario y contraseña en el webmin.

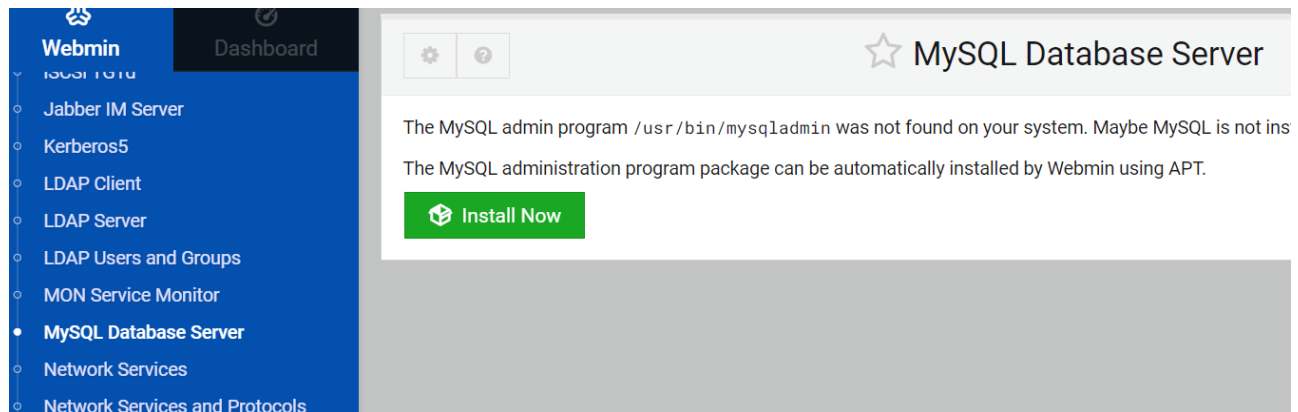


Una vez ingresado los datos se nos muestra una ventana en la que se ven los ajustes y configuración de nuestro administrador web.



Configuraciones para administrar mysql desde webmin

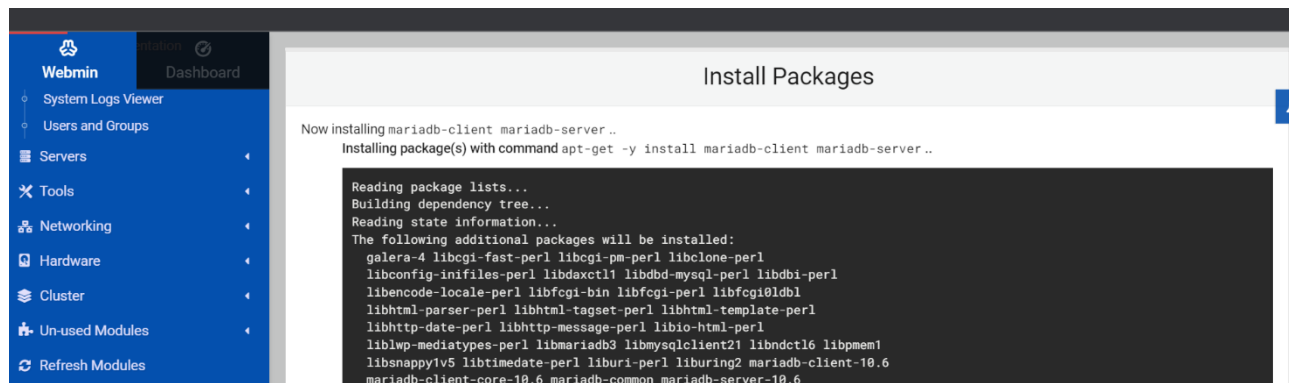
Webmin permite que podamos administrar nuestra base de datos, esto nos da un mejor dominio de nuestro servidor gracias a que este permite de forma gráfica, este nos permite crear y ajustar permisos del mismo, para dirigirnos a las configuraciones nos ubicamos a la izquierda donde podemos ver una serie de opciones, luego a módulos no utilizados y luego en servidor de base de datos mysql, al principio nos aparecerá que debemos instalarlo tal como se muestra en la ilustración.



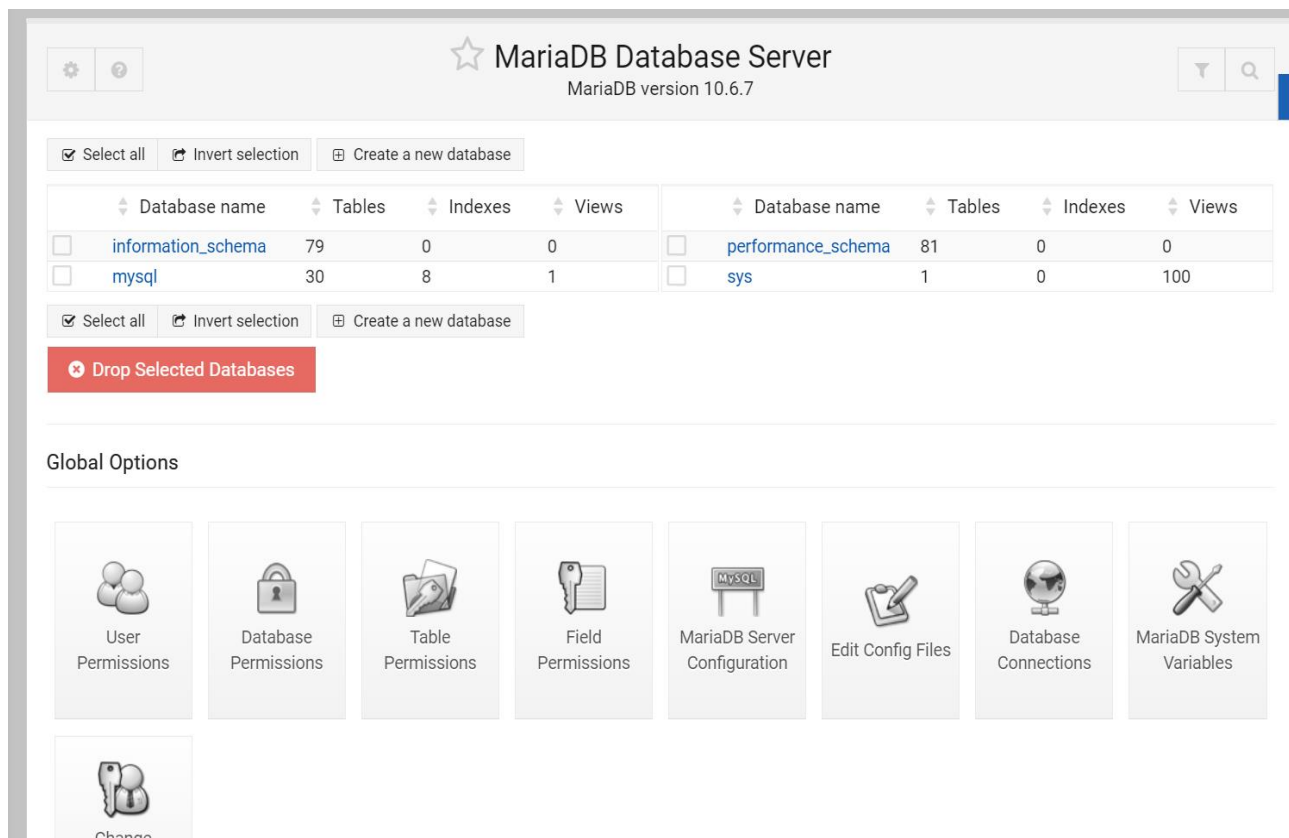
Luego instalamos la lista de paquetes que se nos muestra un total de 36 paquetes en total.



Instalación de los paquetes del servidor mysql.



Una vez instalado todos los 36 paquetes correctamente notamos una ventana con distintas funcionalidades..



Una vez en la ventana oprimimos en crear base de datos para ingresar la información de nuestra base de datos el cual le llamaremos **ExamenPF** y le damos en crear para crear nuestra base de datos MySQL.

Una vez creada se nos muestra en la lista de base de datos que contamos en el servidor

Nombre de la base de datos	Mesas	Índices	Puntos de vista
<input type="checkbox"/> ExamenPF	0	0	0
<input type="checkbox"/> esquema_información	79	0	0
<input type="checkbox"/> mysql	30	8	1

Posterior mente procedemos a configurar los permisos que contara nuestra base de datos, para ello nos dirigimos a la pestaña de **permisos de base de datos**.

Servidor de base de datos MariaDB
MariaDB versión 10.6.7

☒ Seleccionar todo ☐ Invertir selección

Nombre de la base de datos	Mesas	Índices	Puntos de vista
<input checked="" type="checkbox"/> ExamenPF	0	0	0
<input type="checkbox"/> esquema_información	79	0	0
<input type="checkbox"/> mysql	30	8	1

☒ Seleccionar todo ☐ Invertir selección

Opciones globales

Permisos de usuario

Permisos de base de datos

Permisos de tabla

Permisos de campo

Configuración del servidor MariaDB

Editar archivos de configuración

Conexiones de base de datos

Variables del sistema MariaDB

Luego oprimimos dice nuevos permisos de base de datos se nos abrirá una ventana el cual se llenará de la siguiente manera y creamos.

← ? Crear permisos de base de datos

Opciones de permisos de la base de datos

bases de datos ☐ Ningún ☒ Seleccionado ExamenPF ☐ patrón a juego

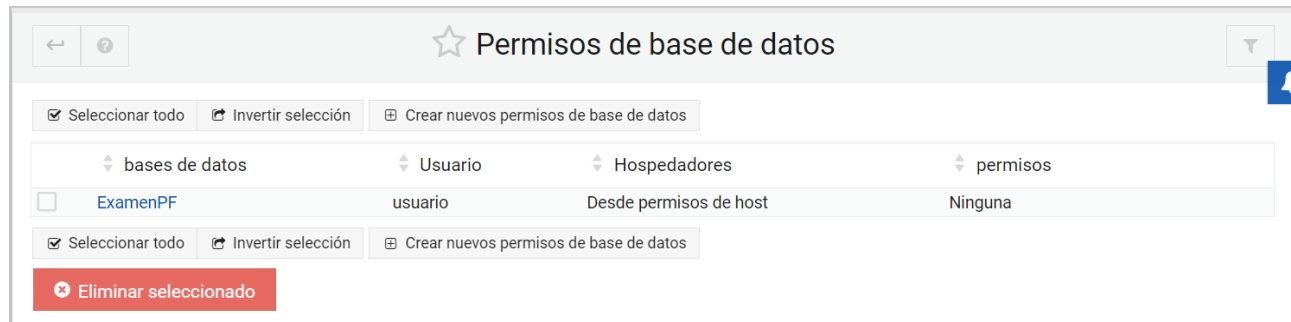
Nombre de usuario ☐ Usuario anónimo ☒ user

Hospedadores ☒ Desde permisos de host ☐ Ningún

permisos

- Seleccionar datos de la tabla
- Insertar datos de tabla
- Actualizar datos de la tabla
- Eliminar datos de la tabla
- Crear tablas
- Caída de mesas

Una vez creada se nos mostrara en la lista de permisos de base de datos de usuarios.



Desarrollo de host virtual

a continuación, se implementará el host virtual para ello ocuparemos con la instalación de WordPress en la que descargaremos e instalaremos para posteriormente ser configurada con una base de dato.

inicialmente accedemos como super usuario con el comando **sudo su**:

```
root@sevidocei:/home/usercei# exit
exit
usercei@sevidocei:~$ sudo su
root@sevidocei:/home/usercei# _
```

posteriormente actualizamos el sistema por recomendación con el comando **apt-get update**, siendo esto recomendable antes de realizar una instalación.

```
root@sevidocei:/home/usercei# sudo su
root@sevidocei:/home/usercei# apt get update
E: Invalid operation get
root@sevidocei:/home/usercei# apt-get update
Obj:1 http://pa.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://pa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Des:3 http://pa.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Des:4 http://pa.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:5 http://pa.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [375 kB]
Des:6 http://pa.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [171 kB]
Ign:7 http://download.webmin.com/download/repository sarge InRelease
Obj:8 http://download.webmin.com/download/repository sarge Release
Descargados 870 kB en 6s (147 kB/s)
Reading package lists... Done
W: http://download.webmin.com/download/repository/dists/sarge/Release.gpg: Key is stored in legacy t
trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
root@sevidocei:/home/usercei# _
```

Procedemos a la instalación del conjunto de servidores LAMP (Linux, Apache, Mysql, php), con el comando **apt-get install apache2 links**.

```
root@sevidocei:/home/usercei# sudo apt-get update
Obj:1 http://pa.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://pa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Ign:3 http://download.webmin.com/download/repository sarge InRelease
Obj:4 http://download.webmin.com/download/repository sarge Release
Des:6 http://pa.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Des:7 http://pa.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Descargados 324 kB en 1s (349 kB/s)
Reading package lists... Done
W: http://download.webmin.com/download/repository/dists/sarge/Release.gpg: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
root@sevidocei:/home/usercei# apt-get install apache2 links_
```

Ejecución de comprobación de estados con el comando **systemctl status apache2** para salir oprimimos **q**

```
root@sevidocei:/home/usercei# systemctl status apache2
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-07-15 05:13:04 UTC; 7min ago
     Docs: https://httpd.apache.org/docs/2.4/
  Process: 637 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
 Main PID: 758 (apache2)
    Tasks: 55 (limit: 1033)
   Memory: 7.5M
      CPU: 76ms
   CGroup: /system.slice/apache2.service
           └─758 /usr/sbin/apache2 -k start
             └─759 /usr/sbin/apache2 -k start
               └─760 /usr/sbin/apache2 -k start

jul 15 05:13:04 sevidocei systemd[1]: Starting The Apache HTTP Server...
jul 15 05:13:04 sevidocei apachectl[692]: AH00558: apache2: Could not reliably determine the serv
jul 15 05:13:04 sevidocei systemd[1]: Started The Apache HTTP Server.
lines 1-17/17 (END)
```

Habilitamos el apache con el comando **systemctl enable apache2**

```
root@sevidocei:/home/usercei# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-in
ll.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@sevidocei:/home/usercei#
```

Restauramos el apache con el comando **systemctl restart apache2**

```
root@sevidocei:/home/usercei# systemctl restart apache2
root@sevidocei:/home/usercei#
```

Instalación de mariadb con el comando **apt-get install mariadb-server**

```
Enabling module mime.
Enabling module negotiation.
Enabling module setenvif.
Enabling module filter.
Enabling module deflate.
Enabling module status.
Enabling module reqtimeout.
Enabling conf charset.
Enabling conf localized-error-pages.
Enabling conf other-vhosts-access-log.
Enabling conf security.
Enabling conf serve-cgi-bin.
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/syste
ache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/s
md/system/apache-htcacheclean.service.
Procesando disparadores para ufw (0.36.1-4build1) ...
Procesando disparadores para man-db (2.10.2-1) ...
Procesando disparadores para libc-bin (2.35-0ubuntu3) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@sevidocei:/home/usercei# apt-get install mariadb-server
```

Comprobación de estado mariadb con el comando **systemctl status mariadb**

```
root@sevidocei:/home/usercei# systemctl status mariadb
● mariadb.service - MariaDB 10.6.7 database server
   Loaded: loaded (/lib/systemd/system/mariadb.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-07-15 05:13:06 UTC; 23min ago
     Docs: man:mariadb(8)
           https://mariadb.com/kb/en/library/systemd/
   Main PID: 753 (mariabdd)
    Status: "Taking your SQL requests now..."
     Tasks: 7 (limit: 1033)
  Memory: 84.2M
     CPU: 763ms
   CGroup: /system.slice/mariadb.service
           └─753 /usr/sbin/mariabdd

jul 15 05:13:05 sevidocei mariabdd[753]: 2022-07-15 5:13:05 0 [Note] Plugin 'FEEDBACK' is disabled.
jul 15 05:13:05 sevidocei mariabdd[753]: 2022-07-15 5:13:05 0 [Note] InnoDB: Buffer pool(s) load c>
jul 15 05:13:05 sevidocei mariabdd[753]: 2022-07-15 5:13:05 0 [Warning] You need to use --log-bin >
jul 15 05:13:05 sevidocei mariabdd[753]: 2022-07-15 5:13:05 0 [Note] Server socket created on IP: >
jul 15 05:13:06 sevidocei mariabdd[753]: 2022-07-15 5:13:06 0 [Note] /usr/sbin/mariabdd: ready for>
jul 15 05:13:06 sevidocei mariabdd[753]: Version: '10.6.7-MariaDB-2ubuntu1' socket: '/run/mysqld/m>
jul 15 05:13:06 sevidocei systemd[1]: Started MariaDB 10.6.7 database server.
jul 15 05:13:06 sevidocei /etc/mysql/debian-start[837]: Upgrading MySQL tables if necessary.
jul 15 05:13:06 sevidocei /etc/mysql/debian-start[848]: Checking for insecure root accounts.
jul 15 05:13:06 sevidocei /etc/mysql/debian-start[852]: Triggering mysam-recover for all MyISAM ta>
lines 1-23/23 (END)
```

Comprobación de habilitación mariadb con el comando **systemctl enable mariadb**

```
Executing: /lib/systemd/systemd-sysv-install enable mariadb
root@sevidocei:/home/usercei#
```

restauramos mariadb con el comando **systemctl restart mariadb**

```
root@sevidocei:/home/usercei# systemctl restart mariadb
root@sevidocei:/home/usercei#
```

accedemos con el comando a nuestra base de datos para asegurarnos de que esta creada con el comando **mysql -u root -p** y para salir escribimos **exit** y le damos en enter.

```
root@sevidocei:/home/usercei# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-2ubuntu1 Ubuntu 22.04

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)]> _
```

Instalamos el módulo de php o complemento php para que tenga conexión con mysql con el comando **apt-get install php php-mysql** y le damos en **S**

```
root@sevidocei:/home/usercei# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-2ubuntu1 Ubuntu 22.04

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)]> exit
Bye
root@sevidocei:/home/usercei# apt-get install php php-mysql
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Se instalarán los siguientes paquetes adicionales:
  libapache2-mod-php8.1 php-common php8.1 php8.1-cli php8.1-common php8.1-mysql php8.1-opcache
  php8.1-readline
Paquetes sugeridos:
  php-pear
Se instalarán los siguientes paquetes NUEVOS:
  libapache2-mod-php8.1 php php-common php-mysql php8.1 php8.1-cli php8.1-common php8.1-mysql
  php8.1-opcache php8.1-readline
0 actualizados, 10 nuevos se instalarán, 0 para eliminar y 24 no actualizados.
Se necesita descargar 5.242 kB de archivos.
Se utilizarán 21,8 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] _
```

Comprobación de configuraciones del complemento php con el comando **nano /var/www/html/info.php**, el cual configuraremos de la siguiente ilustración y guardamos.



```
GNU nano 6.2 /var/www/html/info.php *
<?php
phpinfo();
?>_

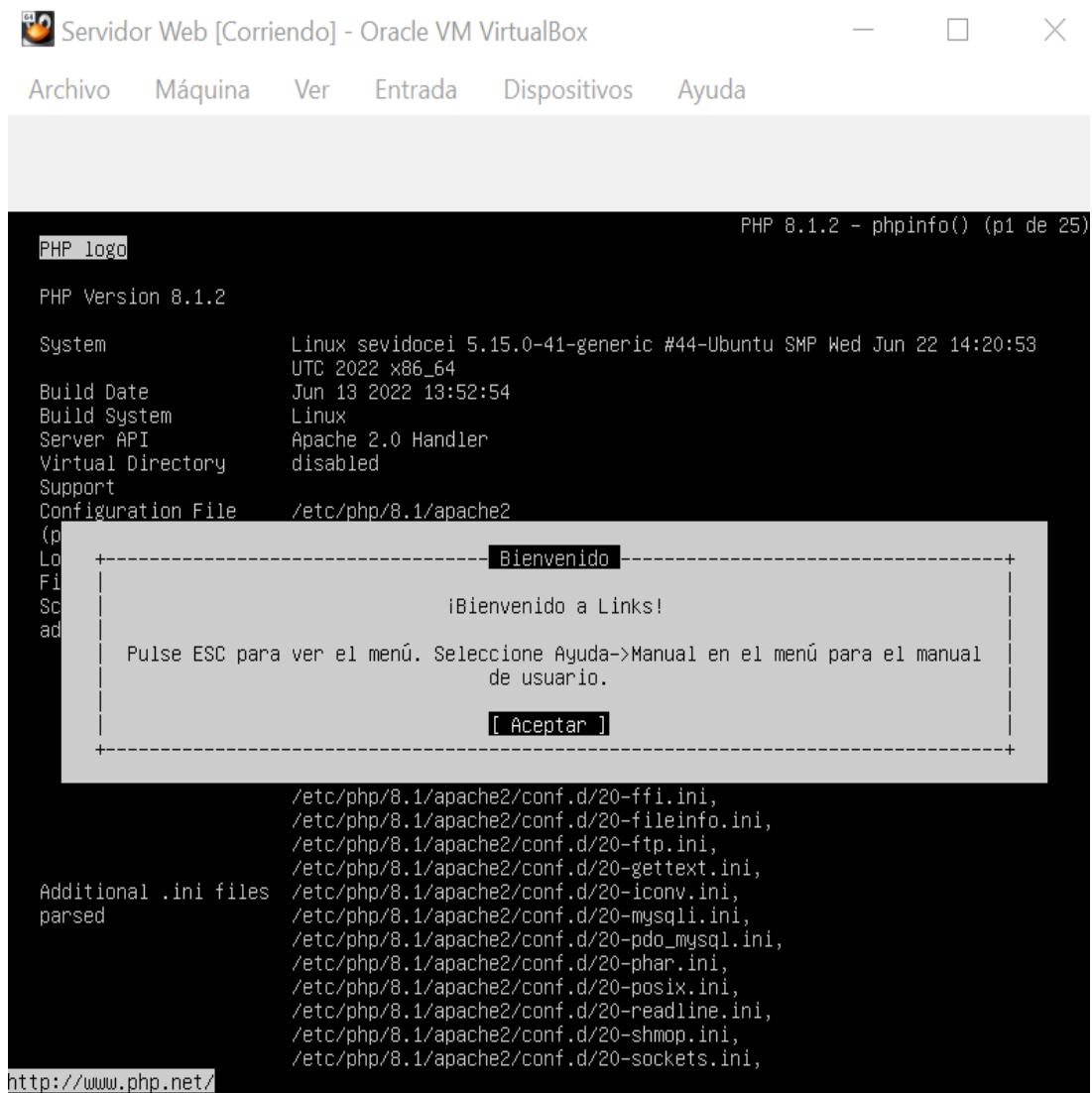
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute  ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify  ^_ Go To Line M-E Redo
```


Configuración del complemento php, este nos permitía realizar a los diagnósticos php.

```
GNU nano 6.2
<?php
phpinfo();
?>
```

Para comprobar la información php y ajustes realizados anteriormente ejecutamos el siguiente comando **links** <http://localhost/info.php> y salimos con **q**

qcd



Actualizamos el sistema para asegurarnos que los paquetes estén con los ajustes más recientes “**apt-get update**”.

```
root@sevidocei:/home/usercei# apt-get update
Obj:1 http://pa.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://pa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Des:3 http://pa.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Des:4 http://pa.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Ign:5 http://download.webmin.com/download/repository sarge InRelease
Obj:6 http://download.webmin.com/download/repository sarge Release
Descargados 324 kB en 6s (58,7 kB/s)
Reading package lists... Done
W: http://download.webmin.com/download/repository/dists/sarge/Release.gpg: Key is stored in legacy trusted.gpg keyring (/etc/apt/trusted.gpg), see the DEPRECATION section in apt-key(8) for details.
root@sevidocei:/home/usercei# _
```

Instalamos el WordPress con el comando **wget https://wordpress.org/latest.zip**

```
root@sevidocei:/home/usercei# wget https://wordpress.org/latest.zip
--2022-07-15 06:59:56-- https://wordpress.org/latest.zip
Resolving wordpress.org (wordpress.org)... 198.143.164.252
Connecting to wordpress.org (wordpress.org)|198.143.164.252|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 22771633 (22M) [application/zip]
Saving to: 'latest.zip'

latest.zip          100%[=====] 21,72M  14,1MB/s   in 1,5s

2022-07-15 06:59:58 (14,1 MB/s) - 'latest.zip' saved [22771633/22771633]

root@sevidocei:/home/usercei# _
```

Instalamos el comando unzip para descomprimir el archivo instalados de wordpress con el siguiente comando **apt-get install unzip**

```
root@sevidocei:/home/usercei# apt-get install unzip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unzip ya está en su versión más reciente (6.0-26ubuntu3).
Unzip fijado como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 24 no actualizados.
root@sevidocei:/home/usercei#
```

Descomprimir el archivo wordpress al directorio /var/www/html con el comando

unzip -q latest.zip -d /var/www/html/

```
root@sevidocei:/home/usercei# unzip -q latest.zip -d /var/www/html/
root@sevidocei:/home/usercei# _
```

verificamos que se descomprimió correctamente con el comando **ls /var/www/html**

```
root@sevidocei:/home/usercei# ls /var/www/html
index.html  info.php  wordpress
root@sevidocei:/home/usercei#
```

ajustamos los permisos de directorio con el comando

chown www-data. -R /var/www/html/wordpress

```
root@sevidocei:/home/usercei# chown www-data. -R /var/www/html/wordpress
root@sevidocei:/home/usercei# _
```

a continuación, configuraremos la base de datos mariadb a WordPress, para ello accedemos a la base de datos mariadb **"mysql -u root -p"**

```
root@sevidocei:/home/usercei# apt-get install unzip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unzip ya está en su versión más reciente (6.0-26ubuntu3).
fijado unzip como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 24 no actualizados.
root@sevidocei:/home/usercei# unzip -q latest.zip -d /var/www/html/
root@sevidocei:/home/usercei# ls /var/www/html
index.html  info.php  wordpress
root@sevidocei:/home/usercei# chown www-data. -R /var/www/html/wordpress
root@sevidocei:/home/usercei# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-2ubuntu1 Ubuntu 22.04

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)]> _
```

creamos la base de datos con distribución de caracteres utf8

“CREATE DATABASE wordpress character set utf8 collate utf8_bin;”

```
root@sevidocei:/home/usercei# apt-get install unzip
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
unzip ya está en su versión más reciente (6.0-26ubuntu3).
Fijado unzip como instalado manualmente.
0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 24 no actualizados.
root@sevidocei:/home/usercei# unzip -q latest.zip -d /var/www/html/
root@sevidocei:/home/usercei# ls /var/www/html
index.html  info.php  wordpress
root@sevidocei:/home/usercei# chown www-data. -R /var/www/html/wordpress
root@sevidocei:/home/usercei# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 31
Server version: 10.6.7-MariaDB-2ubuntu1 Ubuntu 22.04

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 DATABASE wordpress character set utf8 collate utf8_bin;
Query OK, 1 row affected (0.003 sec)

MariaDB [(none)]> _
```

Establecimiento de permisos con la siguiente sintaxis:

GRANT ALL PRIVILEGES on wordpress.* to 'wpuser'@'localhost' identified by 'contraseña';

```
MariaDB [(none)]> GRANT ALL PRIVILEGES on wordpress.* to 'wpuser'@'localhost' identified by 'tuyyo345';
Query OK, 0 rows affected (0.007 sec)

MariaDB [(none)]> _
```

Solicitamos al servidor que aplique las configuraciones con la siguiente sintaxis:

“FLUSH PRIVILEGES;”

```
MariaDB [(none)]> FLUSH PRIVILEGES;
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
```

Verificamos si la base de datos fue creada correctamente “**show databases;**”. Luego ingresamos **exit** para salir

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| ExamenPF |
| information_schema |
| mysql |
| performance_schema |
| sus |
| wordpress |
+-----+
6 rows in set (0.005 sec)

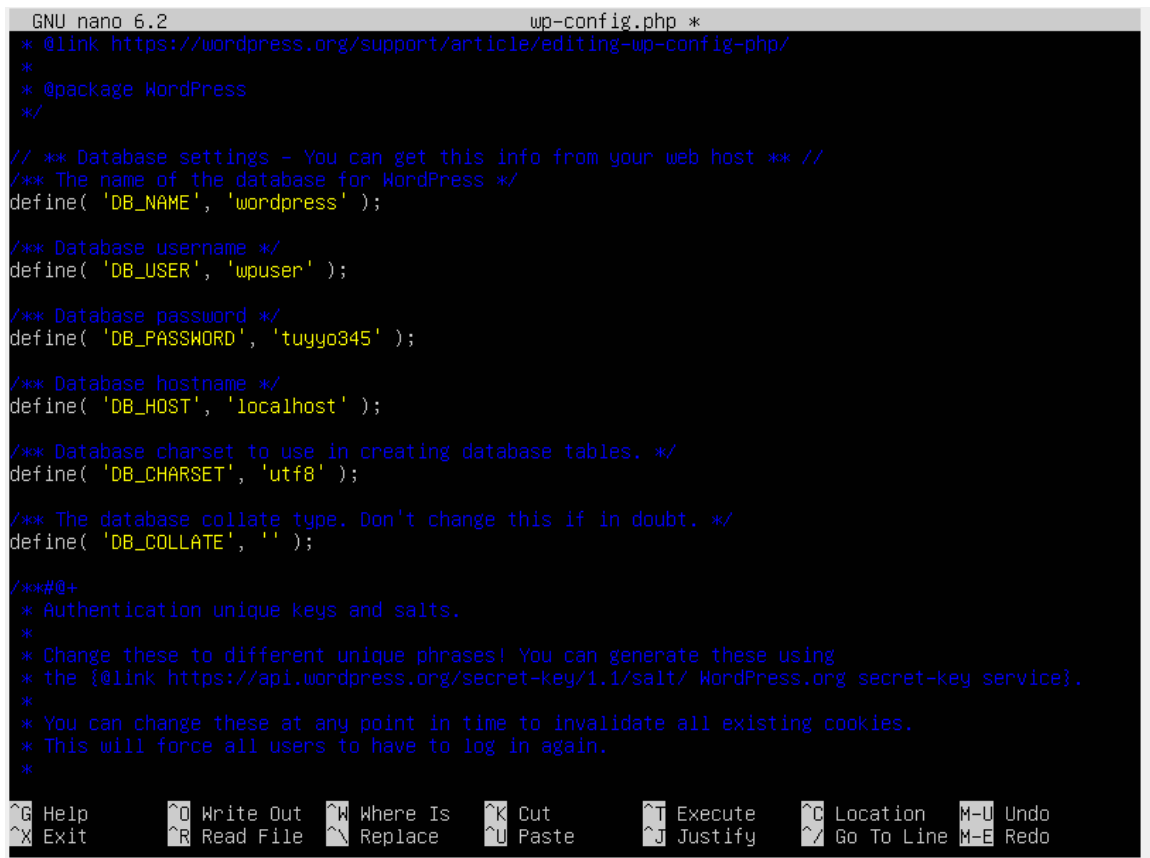
MariaDB [(none)]>
```

Configuración de WordPress

Para la siguiente configuración nos dirigimos al directorio donde se encuentra nuestro archivo WordPress de la siguiente manera. “**cd /var/www/html/wordpress/**”

```
root@sevidocei:/home/usercei# sudo su
root@sevidocei:/home/usercei# cd /var/www/html/wordpress/
root@sevidocei:/var/www/html/wordpress# _
```

Utilizaremos el archivo de configuración que cuenta como ejemplo que en este caso sería: “**mv wp-config-sample.php wp-config.php**” y accedemos con el comando “**nano wp-config.php**” una vez ingresado al archivo se configurara como en la ilustración y guardamos sus cambios.



```
GNU nano 6.2 wp-config.php *
* @link https://wordpress.org/support/article/editing-wp-config-php/
*
* @package WordPress
*/

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wpuser' );

/** Database password */
define( 'DB_PASSWORD', 'tuyyo945' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

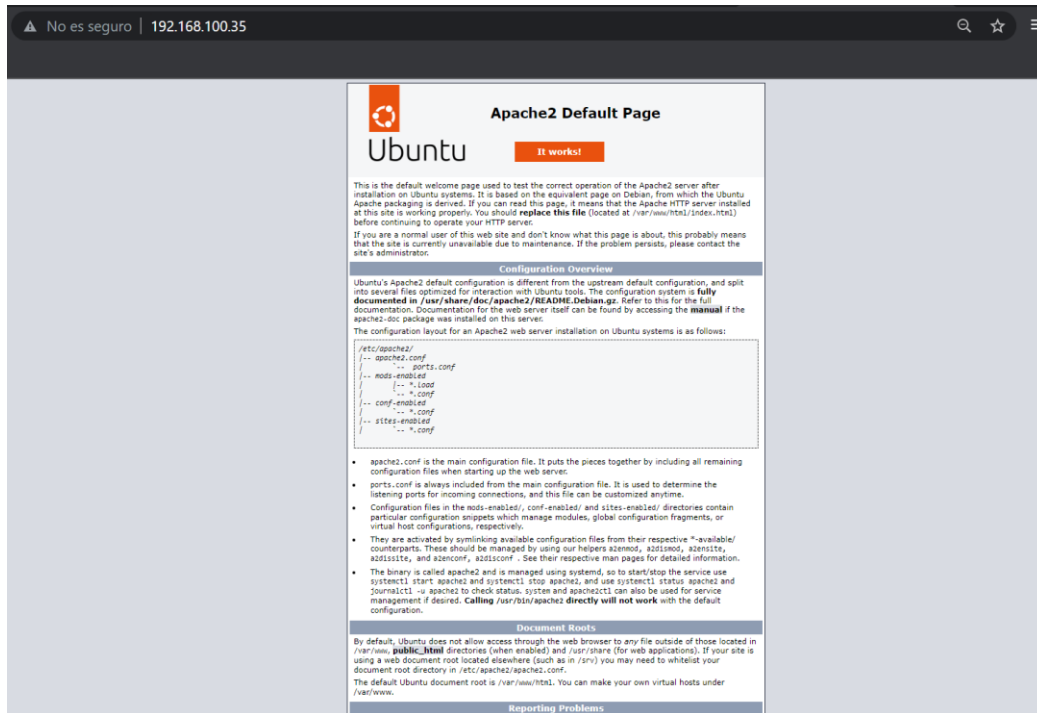
/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

/**#@+
 * Authentication unique keys and salts.
 *
 * Change these to different unique phrases! You can generate these using
 * the {@link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service}.
 *
 * You can change these at any point in time to invalidate all existing cookies.
 * This will force all users to have to log in again.
 */

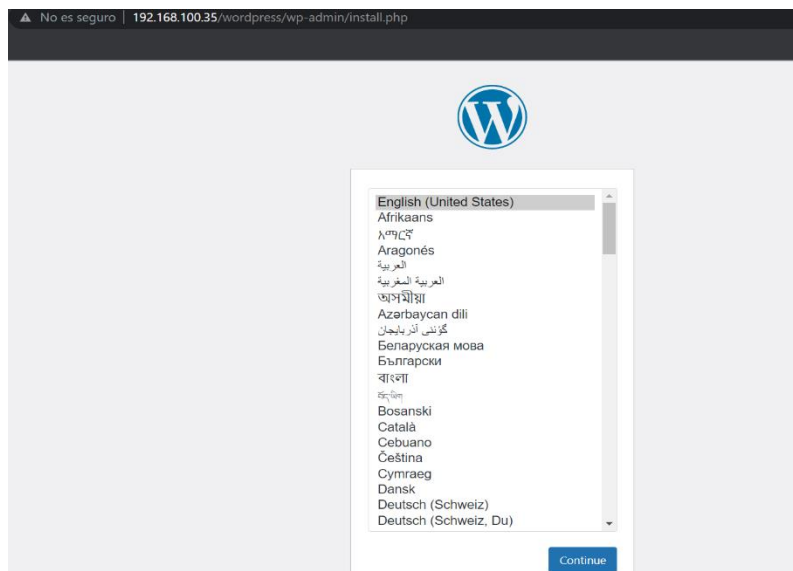
^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location  M-U Undo
^X Exit      ^R Read File ^N Replace   ^U Paste     ^J Justify   ^_ Go To Line M-E Redo
```

Como se puede observar hemos colocado ajustes de la base de datos desarrollado, así como la contraseña el nombre de la base de datos y su nombre de usuario.


Una vez realizado los ajustes perfectamente se nos mostrara en primer lugar una ventana con apache2



Posteriormente procedemos a ingresar al WordPress de la siguiente manera
Ip del servidor/wordpress y se nos mostrara primeramente el ajuste de idioma.



Configuramos los datos de nuestro sitio WordPress y oprimimos en instalar



Hola

¡Bienvenido al 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 [Hide](#)

Strong

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

Tu correo electrónico

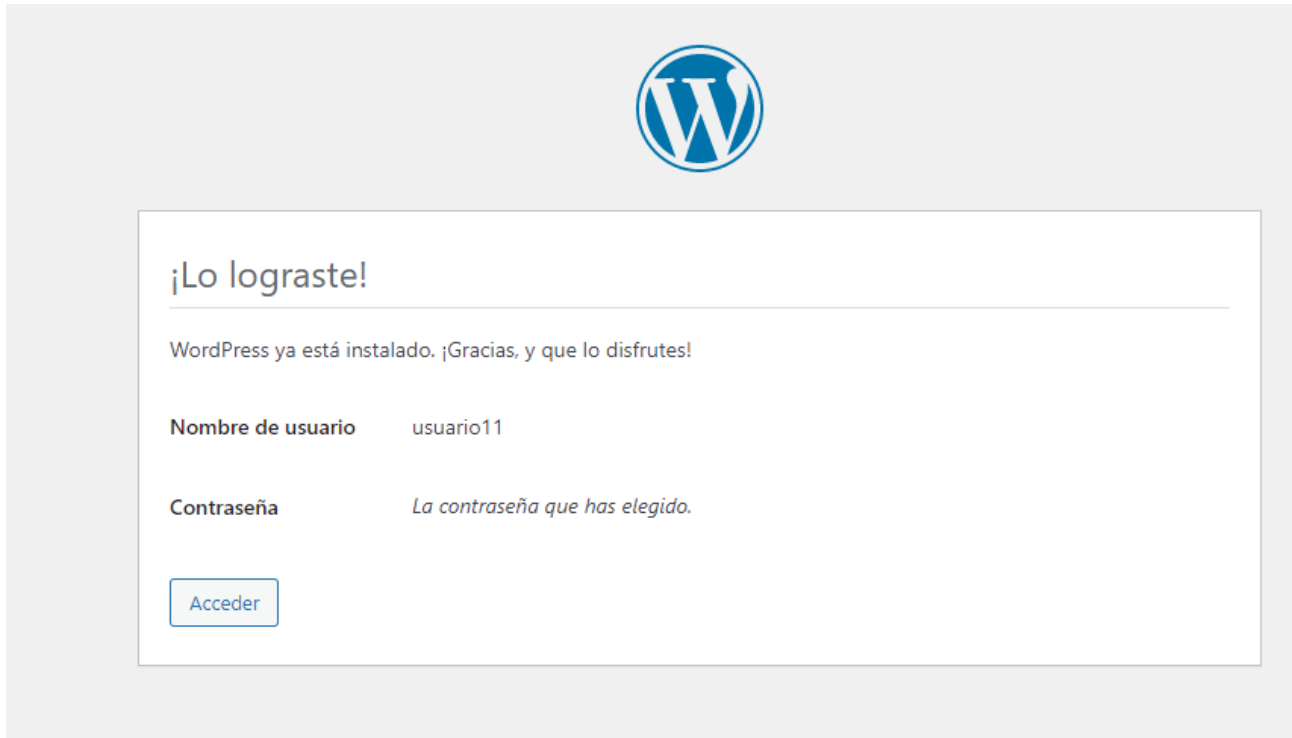
Comprueba bien tu dirección de correo electrónico antes de continuar.

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.

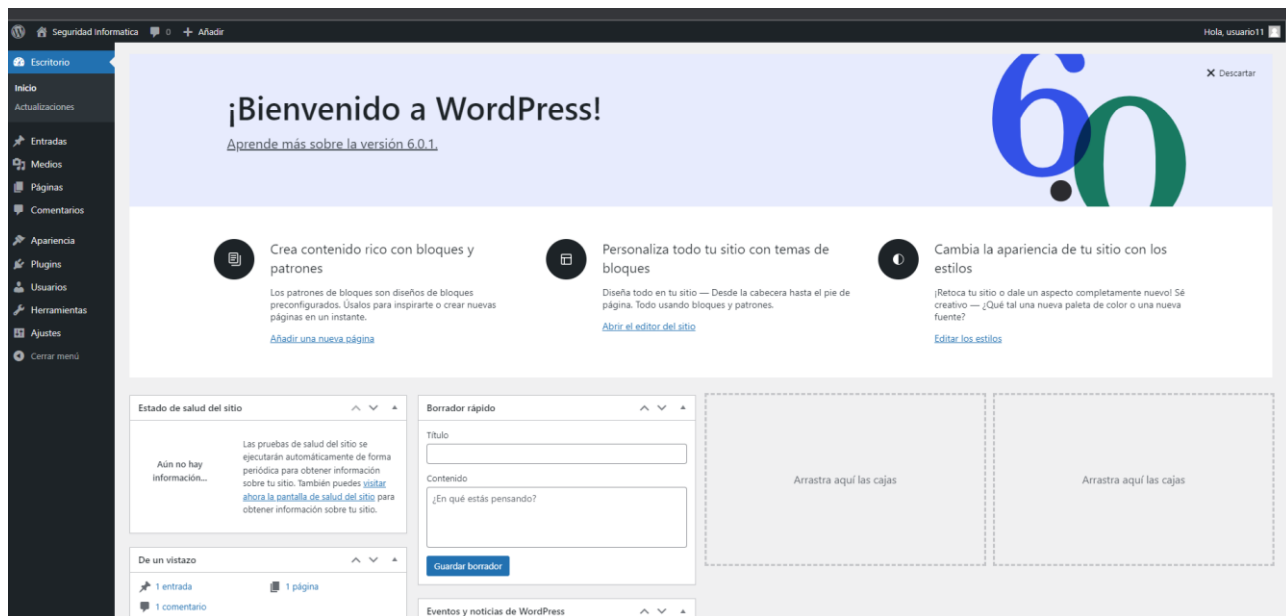
[Instalar WordPress](#)

Nos mostrara que los datos han sido asignados de manera exitosa y accedeos a nuestro sitio web.



Iniciamos sesión





una vez iniciado sesión ya tendríamos nuestro sitio listo, en caso de volver acceder como administrador ingresamos de la siguiente manera: **IP del servidor/wordpress/wp-admin.**

Creación de certificado auto firmado ssh

Como hemos podido observar, accedemos al sitio por medio de una IP y luego colocamos / para accederá nuestro WordPress poque si colocamos solo la IP nos aparece las especificaciones apache, para evitar esto y acceder directamente a nuestro WordPress y acceder por medio de https generaremos un certificado por rsa:2048 con open ssl y una duración de 365 días, para ello ingresaremos el siguiente comando:

```
sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout
/etc/ssl/private/apache-selfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt -out
/etc/ssl/certs/apache-selfsigned.c
```

[illegible]

nos pedirá una serie de datos personales que podemos llenar a nuestro gusto algunos puntos y nos generará una clave o llave, en nuestro caso lo llenamos de la siguiente manera:

[illegible]

A continuación nos dirigimos a al archivo de configuraciones de apache para que utilice las claves generadas, con el siguiente comando: **“sudo vim /etc/apache2/sites-available/default-ssl.conf”**. Una vez accedido al archivo de configuración de apache realizamos los siguientes ajustes que se presentan en la ilustración, no olvidar guardar y salir.

```
<IfModule mod_ssl.c>
```

```
<IfModule mod_ssl.c>
<VirtualHost _default_:443>
    ServerAdmin webmaster@localhost

    DocumentRoot /var/www/html/wordpress
    SSLCertificateFile /etc/ssl/certs/apache-selfsigned.crt
    SSLCertificateKeyFile /etc/ssl/private/apache-selfsigned.key

    # Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
    # error, crit, alert, emerg.
    # It is also possible to configure the loglevel for particular
    # modules, e.g.
    #LogLevel info ssl:warn

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

    # For most configuration files from conf-available/, which are
    # enabled or disabled at a global level, it is possible to
    # include a line for only one particular virtual host. For example the
    # following line enables the CGI configuration for this host only
    # after it has been globally disabled with "a2disconf".
    #Include conf-available/serve-cgi-bin.conf

    #
    # SSL Engine Switch:
    # Enable/Disable SSL for this virtual host.
    SSLEngine on

    #
    # A self-signed (snakeoil) certificate can be created by installing
    # the ssl-cert package. See
    # /usr/share/doc/apache2/README.Debian.gz for more info.
    # If both key and certificate are stored in the same file, only the
    # SSLCertificateFile directive is needed.
    SSLCertificateFile /etc/ssl/certs/ssl-cert-snakeoil.pem
    SSLCertificateKeyFile /etc/ssl/private/ssl-cert-snakeoil.key

```

Como se puede observar en los que este marcado en rojo, hemos configurado la conexión directa a WordPress y hemos agregado las dos llaves generadas anteriormente.

Luego habilitamos las llaves y reiniciamos el servicio apache con los comandos: **sudo a2enmod ssl** y **sudo systemctl restart apache2**. Si al momento de restaurar el apche2 nos muestra un error error debemos desisntalar e instalar nuevamente el apache y vemos el estado con los siguientes comandos:

Primero desinstalar apache2:

```
sudo apt-get purge apache2
```

```
sudo apt-get purge apache2-common
```

```
sudo apt-get purge apache* # this will remove completely
```

```
sudo apt-get update
```

A continuación, instale apache2 nuevo:

```
sudo apt-get install apache2
```

Siguiente Comprobar el estado de apache2

Estado del apache:

```
systemctl status apache2
```

Error del apache al restaurar:

```
root@sevidocei:~# sudo service apache2 start
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
root@sevidocei:~# sudo systemctl restart apache2
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
root@sevidocei:~#
```

Error en el estado de aoache2:

```
root@sevidocei:~# sudo service apache2 start
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
root@sevidocei:~# sudo systemctl restart apache2
Job for apache2.service failed because the control process exited with error code.
See "systemctl status apache2.service" and "journalctl -xeu apache2.service" for details.
root@sevidocei:~# systemctl status apache2
* apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: failed (Result: exit-code) since Fri 2022-07-15 21:35:48 UTC; 1min 56s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 1679 ExecStart=/usr/sbin/apachectl start (code=exited, status=1/FAILURE)
      CPU: 29ms

jul 15 21:35:48 sevidocei systemd[1]: Starting The Apache HTTP Server...
jul 15 21:35:48 sevidocei apachectl[1682]: AH00112: Warning: DocumentRoot [/var/www/wordpress] does not exist
jul 15 21:35:48 sevidocei apachectl[1682]: AH00526: Syntax error on line 6 of /etc/apache2/sites-enabled/000-default.conf: Cannot load modules: /usr/lib/apache2/modules: (dlopen error: /usr/lib/apache2/modules: cannot open shared object file: No such file or directory)
jul 15 21:35:48 sevidocei apachectl[1679]: Action 'start' failed.
jul 15 21:35:48 sevidocei apachectl[1679]: The Apache error log may have more information.
jul 15 21:35:48 sevidocei systemd[1]: apache2.service: Control process exited, code=exited, status=1/FAILURE
jul 15 21:35:48 sevidocei systemd[1]: apache2.service: Failed with result 'exit-code'.
jul 15 21:35:48 sevidocei systemd[1]: Failed to start The Apache HTTP Server.
lines 1-16/16 (END)
```

una vez realizado los pasos anteriores contaremos con nuestro apache2 activado y verificamos el archivo wordpress donde colocamos las llaves si esta todo correcto.

```
Enabling site 000-default.
Created symlink /etc/systemd/system/multi-user.target.wants/apache2.service → /lib/systemd/system/apache2.service.
Created symlink /etc/systemd/system/multi-user.target.wants/apache-htcacheclean.service → /lib/systemd/system/apache-htcacheclean.service.
Procesando disparadores para man-db (2.10.2-1) ...
Procesando disparadores para ufw (0.36.1-4build1) ...
Scanning processes...
Scanning linux images...

Running kernel seems to be up-to-date.

No services need to be restarted.

No containers need to be restarted.

No user sessions are running outdated binaries.

No VM guests are running outdated hypervisor (qemu) binaries on this host.
root@sevidocei:~# systemctl status apache2
* apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Fri 2022-07-15 21:44:36 UTC; 16s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Main PID: 5909 (apache2)
      Tasks: 55 (limit: 1033)
     Memory: 4.7M
        CPU: 32ms
    CGroup: /system.slice/apache2.service
            └─5909 /usr/sbin/apache2 -k start
              └─5911 /usr/sbin/apache2 -k start
                └─5912 /usr/sbin/apache2 -k start

jul 15 21:44:36 sevidocei systemd[1]: Starting The Apache HTTP Server...
jul 15 21:44:36 sevidocei apachectl[5908]: AH00558: apache2: Could not reliably determine the server's fully qualified domain name, please add the 'ServerName' directive with the fully qualified domain name of the server.
jul 15 21:44:36 sevidocei systemd[1]: Started The Apache HTTP Server.
lines 1-16/16 (END)
```

habilitamos las llaves y reiniciamos el servicio apache con los comandos: **sudo a2enmod ssl** y **sudo systemctl restart apache2**.

```
root@sevidocei:~# sudo a2enmod ssl
Considering dependency setenvif for ssl:
Module setenvif already enabled
Considering dependency mime for ssl:
Module mime already enabled
Considering dependency socache_shmcb for ssl:
Enabling module socache_shmcb.
Enabling module ssl.
See /usr/share/doc/apache2/README.Debian.gz on how to configure SSL and create self-signed certificates.
To activate the new configuration, you need to run:
    systemctl restart apache2
root@sevidocei:~# sudo systemctl restart apache2
root@sevidocei:~# _
```

Habilitamos el ssl para el sitio web “**sudo a2ensite default-ssl**” y reinicioamos reiniciamos con el comando **sudo systemctl reload apache2**

```
root@sevidocei:~# sudo a2ensite default-ssl
Enabling site default-ssl.
To activate the new configuration, you need to run:
    systemctl reload apache2
root@sevidocei:~# sudo systemctl reload apache2
root@sevidocei:~#
```

Accedemos al archivo de apache2 con el comando: **sudo vim /etc/apache2/sites-available/000-default.conf** y lo editamos de la siguiente manera.

```
<VirtualHost *:80>
# The ServerName directive sets the request scheme, hostname and port that
# the server uses to identify itself. This is used when creating
# redirection URLs. In the context of virtual hosts, the ServerName
# specifies what hostname must appear in the request's Host: header to
# match this virtual host. For the default virtual host (this file) this
# value is not decisive as it is used as a last resort host regardless.
# However, you must set it for any further virtual host explicitly.
#ServerName www.example.com

ServerAdmin webmaster@localhost
DocumentRoot /var/www/html/wordpress
Servername localhost

# Available loglevels: trace8, ..., trace1, debug, info, notice, warn,
# error, crit, alert, emerg.
# It is also possible to configure the loglevel for particular
# modules, e.g.
#LogLevel info ssl:warn

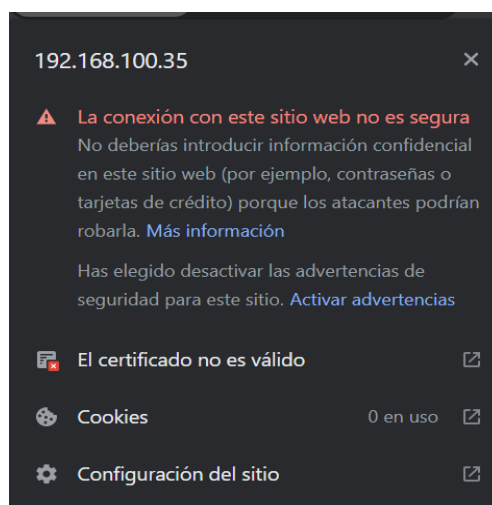
ErrorLog ${APACHE_LOG_DIR}/error.log
CustomLog ${APACHE_LOG_DIR}/access.log combined

# For most configuration files from conf-available/, which are
# enabled or disabled at a global level, it is possible to
# include a line for only one particular virtual host. For example the
# following line enables the CGI configuration for this host only
# after it has been globally disabled with "a2disconf".
#Include conf-available/serve-cgi-bin.conf
</VirtualHost>

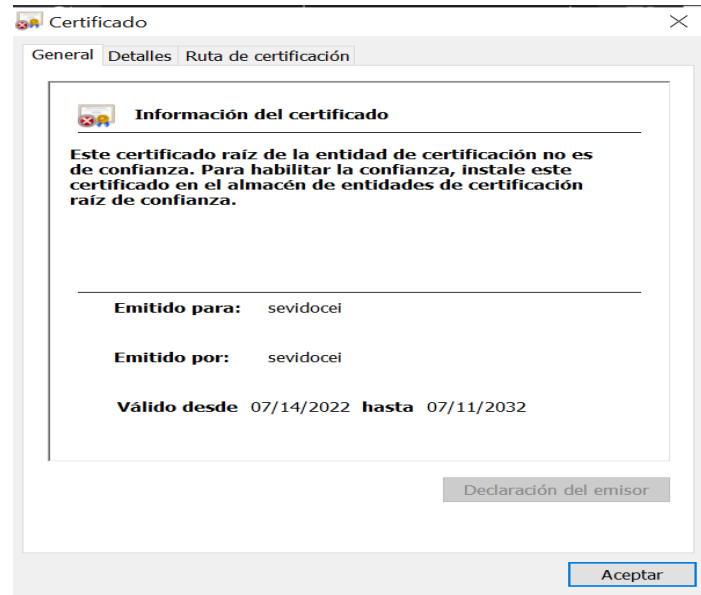
# vim: syntax=apache ts=4 sw=4 sts=4 sr noet

-- INSERTAR --
```

Para confirmar que nuestro certificado a sido implementado perfectamente nos dirigimos a la pestaña del sitio web como se muestra a continuación e ingresamos a certificado no validado.



Una vez ingresado podemos ver las especificaciones y detalles que ingresamos después de haber ejecutado el comando generado de llaves como se muestra a continuación.



Instalación de Redis

A continuación se procede a instalar el almacén de estructuras de datos Redis, para potenciar nuestro WordPress, para ello partiremos desde la instalación de los paquetes de Redis con el comando `sudo apt-get install redis-server php.redis` y comisarará con la instalación, luego nos pregunta si deseamos continuar y le damos que S y enter.

```
g++ g++-11 gcc gcc-11 gcc-11-base gettext intltool-debian libalgorithm-diff-perl
libalgorithm-diff-xs-perl libalgorithm-merge-perl libarchive-cpio-perl libarchive-zip-perl
libasan6 libatomic1 libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libdebhelper-perl
libdeflate0 libdpkg-perl libfakeroot libfile-fcntllock-perl libfile-stripnondeterminism-perl
libfontconfig1 libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjbig0 libjemalloc2
libjpeg-turbo8 libjpeg8 liblsan0 libltdl-dev libltdl7 liblua5.1-0 liblzfl1 libmail-sendmail-perl
libmpc3 libnsl-dev libonig5 libpcre2-16-0 libpcre2-32-0 libpcre2-dev libpcre2-posix3
libquadmath0 libssl-dev libstdc++-11-dev libsub-override-perl libsys-hostname-long-perl libtiff5
libtirpc-dev libtool libtsan0 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list
lua-bitop lua-cjson m4 make manpages-dev php-all-dev php-igbinary-all-dev php-json php-pear
php-xml php8.1-dev php8.1-igbinary php8.1-mbstring php8.1-redis php8.1-xml pkg-config
pkg-php-tools po-debconf redis-tools rpcsvc-proto shtool
paquetes sugeridos:
autoconf-archive gnu-stardards autoconf-doc cpp-doc gcc-11-locales dh-make debian-keyring
g++-multilib g++-11-multilib gcc-11-doc gcc-multilib flex bison gdb gcc-doc gcc-11-multilib
gettext-doc libasprintf-dev libgettextpo-dev glibc-doc bzip2 libgd-tools libtool-doc libssl-dev
libstdc++-11-doc gfortran | fortan95-compiler gcj-jdk m4-doc make-doc dh-php libmail-box-perl
ruby-redis
e instalarán los siguientes paquetes NUEVOS:
autoconf automake autopoint autotools-dev build-essential cpp cpp-11 debhelper debugedit
dh-autoreconf dh-strip-nondeterminism dpkg-dev dwz fakeroot fontconfig-config fonts-dejavu-core
g++ g++-11 gcc gcc-11 gcc-11-base gettext intltool-debian libalgorithm-diff-perl
libalgorithm-diff-xs-perl libalgorithm-merge-perl libarchive-cpio-perl libarchive-zip-perl
libasan6 libatomic1 libc-dev-bin libc-devtools libc6-dev libcc1-0 libcrypt-dev libdebhelper-perl
libdeflate0 libdpkg-perl libfakeroot libfile-fcntllock-perl libfile-stripnondeterminism-perl
libfontconfig1 libgcc-11-dev libgd3 libgomp1 libisl23 libitm1 libjbig0 libjemalloc2
libjpeg-turbo8 libjpeg8 liblsan0 libltdl-dev libltdl7 liblua5.1-0 liblzfl1 libmail-sendmail-perl
libmpc3 libnsl-dev libonig5 libpcre2-16-0 libpcre2-32-0 libpcre2-dev libpcre2-posix3
libquadmath0 libssl-dev libstdc++-11-dev libsub-override-perl libsys-hostname-long-perl libtiff5
libtirpc-dev libtool libtsan0 libubsan1 libwebp7 libxpm4 linux-libc-dev lto-disabled-list
lua-bitop lua-cjson m4 make manpages-dev php-all-dev php-igbinary-all-dev php-json php-pear
php-redis php-redis-all-dev php-xml php8.1-dev php8.1-igbinary php8.1-mbstring php8.1-redis
php8.1-xml pkg-config pkg-php-tools po-debconf redis-server redis-tools rpcsvc-proto shtool
actualizados, 102 nuevos se instalarán, 0 para eliminar y 32 no actualizados.
e necesita descargar 74,8 MB de archivos.
e utilizarán 254 MB de espacio de disco adicional después de esta operación.
¿desea continuar? [S/n] ^[S]
```


Instalación de Redis en progreso.

```
Servidor Web [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
Des:16 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libpcre2-dev amd64 10.39-3build1 [727 kB]
Des:17 http://pa.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libssl-dev amd64 3.0.2-0ubuntu1.1 [2,370 kB]
Des:18 http://pa.archive.ubuntu.com/ubuntu jammy-updates/main amd64 libdpkg-perl all 1.21.1ubuntu2.1 [237 kB]
Des:19 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 pkg-config amd64 0.29.2-1ubuntu3 [48,2 kB]
Des:20 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 shtool all 2.0.8-10 [122 kB]
Des:21 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 gcc-11-base amd64 11.2.0-19ubuntu1 [20,8 kB]
Des:22 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libisl23 amd64 0.24-2build1 [727 kB]
Des:23 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libmpc3 amd64 1.2.1-2build1 [46,9 kB]
Des:24 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 cpp-11 amd64 11.2.0-19ubuntu1 [9,966 kB]
Des:25 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 cpp amd64 4:11.2.0-1ubuntu1 [27,7 kB]
Des:26 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libcc1-0 amd64 12-20220319-1ubuntu1 [47,2 kB]
Des:27 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libgomp1 amd64 12-20220319-1ubuntu1 [126 kB]
Des:28 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libitm1 amd64 12-20220319-1ubuntu1 [30,2 kB]
Des:29 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libatomic1 amd64 12-20220319-1ubuntu1 [10,4 kB]
Des:30 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libasan6 amd64 11.2.0-19ubuntu1 [2,283 kB]
Des:31 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 liblsan0 amd64 12-20220319-1ubuntu1 [1,069 kB]
Des:32 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libtsan0 amd64 11.2.0-19ubuntu1 [2,261 kB]
Des:33 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libubsan1 amd64 12-20220319-1ubuntu1 [976 kB]
Des:34 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libquadmath0 amd64 12-20220319-1ubuntu1 [154 kB]
Des:35 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 libgcc-11-dev amd64 11.2.0-19ubuntu1 [2,526 kB]
Des:36 http://pa.archive.ubuntu.com/ubuntu jammy/main amd64 gcc-11 amd64 11.2.0-19ubuntu1 [20,1 MB]
43% [36 gcc-11 4.496 kB/20,1 MB 22%] 394 kB/s 1min 44s
```

Una vez instalado los paquetes, comprobamos que funcione perfectamente con el comando **redis-cli** y luego el comando **ping** y si nos da primeramente una IP y una respuesta pong nos esta indicando que funcionando perfectamente y salimos con **exit**.

```
root@sevidocei:/home/usercei# redis-cli
127.0.0.1:6379> ping
PONG
127.0.0.1:6379> exit
root@sevidocei:/home/usercei# _
```

Ingresamos a la configuración de la memoria máxima de reglas para Redis con el comando **sudo vim /etc/redis/redis.conf**

```
# Redis configuration file example.
#
# Note that in order to read the configuration file, Redis must be
# started with the file path as first argument:
#
# ./redis-server /path/to/redis.conf
#
# Note on units: when memory size is needed, it is possible to specify
# it in the usual form of 1k 5GB 4M and so forth:
#
# 1k => 1000 bytes
# 1kb => 1024 bytes
# 1m => 1000000 bytes
# 1mb => 1024*1024 bytes
# 1g => 1000000000 bytes
# 1gb => 1024*1024*1024 bytes
#
# units are case insensitive so 1GB 1Gb 1gB are all the same.
##### INCLUDES #####
#
# Include one or more other config files here. This is useful if you
# have a standard template that goes to all Redis servers but also need
# to customize a few per-server settings. Include files can include
# other files, so use this wisely.
#
# Note that option "include" won't be rewritten by command "CONFIG REWRITE"
# from admin or Redis Sentinel. Since Redis always uses the last processed
# line as value of a configuration directive, you'd better put includes
# at the beginning of this file to avoid overwriting config change at runtime.
```

Una vez ingresado al archivo para ajustar los límites de memoria de almacenamiento de información Mysql, una vez en el archivo nos ubicamos o nos desplazamos hacia abajo donde se encuentra la instrucción maxmemory que se encuentra comentado y ubicado en la sección del archivo **MEMORY MANAGMENT**, .

```
##### MEMORY MANAGEMENT #####
# Set a memory usage limit to the specified amount of bytes.
# When the memory limit is reached Redis will try to remove keys
# according to the eviction policy selected (see maxmemory-policy).
#
# If Redis can't remove keys according to the policy, or if the policy is
# set to 'noeviction', Redis will start to reply with errors to commands
# that would use more memory, like SET, LPUSH, and so on, and will continue
# to reply to read-only commands like GET.
#
# This option is usually useful when using Redis as an LRU or LFU cache, or to
# set a hard memory limit for an instance (using the 'noeviction' policy).
#
# WARNING: If you have replicas attached to an instance with maxmemory on,
# the size of the output buffers needed to feed the replicas are subtracted
# from the used memory count, so that network problems / resyncs will
# not trigger a loop where keys are evicted, and in turn the output
# buffer of replicas is full with DELs of keys evicted triggering the deletion
# of more keys, and so forth until the database is completely emptied.
#
# In short... if you have replicas attached it is suggested that you set a lower
# limit for maxmemory so that there is some free RAM on the system for replica
# output buffers (but this is not needed if the policy is 'noeviction').
#
# maxmemory <bytes>
#
# MAXMEMORY POLICY: how Redis will select what to remove when maxmemory
# is reached. You can select one from the following behaviors:
#
# volatile-lru -> Evict using approximated LRU, only keys with an expire set.
# allkeys-lru -> Evict any key using approximated LRU.
```

Luego procedemos a ajustar la memoria, en este caso le asignaremos a 256 mb, para editarlo oprimimos la tecla **insert** y des comentamos la instrucción y para guardar mantenemos presionado la tecla **esc** escribimos dos puntos wq y enter una vez quede ajustado tal como se muestra en la siguiente ilustración.

```
##### MEMORY MANAGEMENT #####
# Set a memory usage limit to the specified amount of bytes.
# When the memory limit is reached Redis will try to remove keys
# according to the eviction policy selected (see maxmemory-policy).
#
# If Redis can't remove keys according to the policy, or if the policy is
# set to 'noeviction', Redis will start to reply with errors to commands
# that would use more memory, like SET, LPUSH, and so on, and will continue
# to reply to read-only commands like GET.
#
# This option is usually useful when using Redis as an LRU or LFU cache, or to
# set a hard memory limit for an instance (using the 'noeviction' policy).
#
# WARNING: If you have replicas attached to an instance with maxmemory on,
# the size of the output buffers needed to feed the replicas are subtracted
# from the used memory count, so that network problems / resyncs will
# not trigger a loop where keys are evicted, and in turn the output
# buffer of replicas is full with DELs of keys evicted triggering the deletion
# of more keys, and so forth until the database is completely emptied.
#
# In short... if you have replicas attached it is suggested that you set a lower
# limit for maxmemory so that there is some free RAM on the system for replica
# output buffers (but this is not needed if the policy is 'noeviction').
#
# maxmemory 256mb
#
# MAXMEMORY POLICY: how Redis will select what to remove when maxmemory
# is reached. You can select one from the following behaviors:
#
```

Reiniciando Redis

```
root@sevidocei:/home/usercei# sudo systemctl restart redis-server
root@sevidocei:/home/usercei# _
```

Accediendo a las configuraciones de WordPress, para este caso nuestra configuración WordPress esta ubicada en la dirección para ello dos dirigimos a la dirección en donde se encuentra ubicado de la siguiente manera: “**cd /var/www/html/wordpress**”

```
root@sevidocei:~# cd /var/www/html/wordpress
root@sevidocei:/var/www/html/wordpress# _
```

Posteriormente una vez que nos hemos dirigido al directorio ingresamos el siguiente comando: “**vim wp-config.php**” para acceder a el archivo de configuración de WordPress y lo ajustamos el archivo en la sección como se muestra a continuación y guardamos oprimiendo **esc** y escribiendo **dos puntos wq** y oprimimos **enter**.

```
* * Secret keys
* * Database table prefix
* * ABSPATH
*
* @link https://wordpress.org/support/article/editing-wp-config-php/
*
* @package WordPress
*/

// ** Database settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define( 'DB_NAME', 'wordpress' );

/** Database username */
define( 'DB_USER', 'wpuser' );

/** Database password */
define( 'DB_PASSWORD', 'tuyyo345' );

/** Database hostname */
define( 'DB_HOST', 'localhost' );

/** Database charset to use in creating database tables. */
define( 'DB_CHARSET', 'utf8' );

/** The database collate type. Don't change this if in doubt. */
define( 'DB_COLLATE', '' );

define( 'WP_CACHE', verdadero );
define( 'WP_CACHE_KEY_SALT', 'rediswp.com' );

/*#@+
 * Authentication unique keys and salts.
 *
 * Change these to different unique phrases! You can generate these using
 * the @link https://api.wordpress.org/secret-key/1.1/salt/ WordPress.org secret-key service
 */
```

Es importante considerar la sección de **cahe key salt** ya que esta es la parte en la que colocamos nuestro dominio del WordPress por lo que nuestro WordPress debe contar con un dominio antes de colocar esta instrucción. Posteriormente nos dirigimos a nuestro WordPress como administrador y luego a plugins y en añadir plugins y e buscar escribimos Redis y nos debe aparecer un plugin como se muestra en la ilustración y le damos en instalar

Mod security

Primero necesitamos actualizar el sistema con la última versión. Ejecutamos los siguientes comandos:

- `apt-get update -y`
- `apt-get upgrade -y`

```
root@servidocei:/home/usercei# apt-get update -y
Obj:1 http://pa.archive.ubuntu.com/ubuntu jammy InRelease
Des:2 http://pa.archive.ubuntu.com/ubuntu jammy-updates InRelease [114 kB]
Des:3 http://pa.archive.ubuntu.com/ubuntu jammy-backports InRelease [99,8 kB]
Des:4 http://pa.archive.ubuntu.com/ubuntu jammy-security InRelease [110 kB]
Des:5 http://pa.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [375 kB]
Des:6 http://pa.archive.ubuntu.com/ubuntu jammy-updates/universe amd64 Packages [171 kB]
Descargados 870 kB en 3s (326 kB/s)
Reading package lists... Done
root@servidocei:/home/usercei#
```

`apt-get install apache2 mysql-server libapache2-mod-auth-mysql php5-mysql php5 libapache2-mod-php5 php5-mcrypt`

Una vez hecha las instalaciones anteriores, reiniciamos apache2

- `systemctl start apache2`
- `systemctl enable apache2`

```
root@servidocei:/home/usercei# systemctl start apache2
root@servidocei:/home/usercei# systemctl enable apache2
Synchronizing state of apache2.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable apache2
root@servidocei:/home/usercei# _
```

Execution del commando: **apt-get install libapache2-modsecurity**

```
root@servidocei:/home/usercei# apt-get install libapache2-modsecurity
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
root@servidocei:/home/usercei#
```

Después de haber hecho la instalación podemos verificar con el siguiente comando:

apachectl -M | grep security

```
root@servidocei:/home/usercei# apachectl -M | grep security
AH00558: apache2: Could not reliably determine the server's fully qualified domain na
.1.1. Set the 'ServerName' directive globally to suppress this message
root@servidocei:/home/usercei# _
```

realizando configuraciones con el comando: **mv /etc/modsecurity/modsecurity.conf-recommended /etc/modsecurity/modsecurity.conf**

Con figuramos el archivo mod securut accediendo con el comando: **nano /etc/modsecurity/modsecurity.conf**

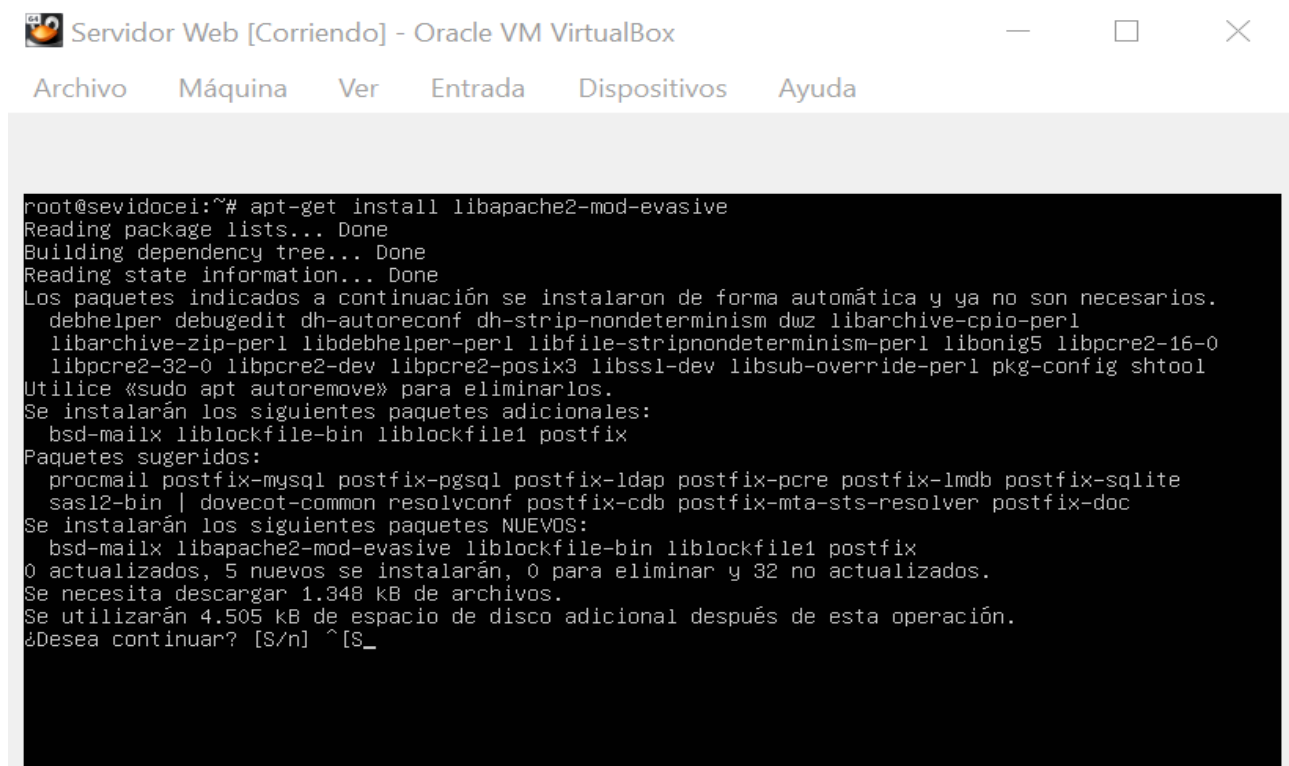
Cambiamos las siguientes líneas:

```
GNU nano 2.5.3      File: /etc/modsecurity/modsecurity.conf      Modified

# -- Rule engine initialization -----
# Enable ModSecurity, attaching it to every transaction. Use detection
# only to start with, because that minimises the chances of post-installation
# disruption.
#
#secRuleEngine DetectionOnly
SecRuleEngine on
```

Instalación de mod evasive

Ejecutamos el siguiente comando: **apt-get install libapache2-mod-evasive** y oprimimos **s** para continuar.



```
root@sevidocei:~# apt-get install libapache2-mod-evasive
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
  debhelper debugedit dh-autoreconf dh-strip-nondeterminism dwz libarchive-cpio-perl
  libarchive-zip-perl libdebhelper-perl libfile-stripnondeterminism-perl libonig5 libpcre2-16-0
  libpcre2-32-0 libpcre2-dev libpcre2-posix3 libssl-dev libsub-override-perl pkg-config shtool
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
  bsd-mailx liblockfile-bin liblockfile1 postfix
Paquetes sugeridos:
  procmail postfix-mysql postfix-pgsql postfix-ldap postfix-pcre postfix-lmdb postfix-sqlite
  sasl2-bin | dovecot-common resolvconf postfix-cdb postfix-mta-sts-resolver postfix-doc
Se instalarán los siguientes paquetes NUEVOS:
  bsd-mailx libapache2-mod-evasive liblockfile-bin liblockfile1 postfix
0 actualizados, 5 nuevos se instalarán, 0 para eliminar y 32 no actualizados.
Se necesita descargar 1.348 kB de archivos.
Se utilizarán 4.505 kB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] ^[S_
```

Creamos la carpeta o directorio de logs `mkdir /var/log/mod_evasive` y posteriormente le Cambiamos el dueño de la carpeta `chown www-data:www-data /var/log/mod_evasive/`



```
root@sevidocei:~# mkdir /var/log/mod_evasive
root@sevidocei:~# chown www-data:www-data /var/log/mod_evasive
root@sevidocei:~# _
```

Conclusión

Culminado este curso hemos adquirido nuevos conocimientos ya que al principio se nos hizo muy complicado debido a que no manejábamos muy bien los términos y sobre todo la parte práctica del sistema operativo que estábamos utilizando, Ubuntu server que para en este proyecto realizamos un web server, recreando las condiciones del mundo real. El servidor web utilizado para la experiencia fue un servidor Ubuntu versión 22.04.5. Haciendo uso de una máquina virtual Linux. Aplicamos los conceptos aprendidos a lo largo del semestre para detectar fallos comunes, evitarlos y mejorar la seguridad del servidor web. Al servidor web le instalamos los servicios LAMP y OpenSSH. Lo cual figura como aplicación de cifrado de las comunicaciones en la red, haciendo uso del protocolo SSH. Procedemos a crear el sitio web, por lo que hacemos uso de las aplicaciones Webmin, Wordpres

Referencias

- cloudflare*. (2022). Obtenido de <https://www.cloudflare.com/es-es/learning/ddos/ddos-attack-tools/slowloris/>
- dinahosting*. (s.f.). Obtenido de [https://dinahosting.com/ayuda/excepciones-de-mod_security/#:~:text=mod_security%20es%20un%20m%C3%B3dulo%20de,SQL%20\(SQLi\)%2C%20etc.](https://dinahosting.com/ayuda/excepciones-de-mod_security/#:~:text=mod_security%20es%20un%20m%C3%B3dulo%20de,SQL%20(SQLi)%2C%20etc.)
- IBM.com*. (s.f.). Obtenido de <https://www.ibm.com/docs/es/aix/7.1?topic=protocol-tcpip-network-interfaces>
- linube*. (s.f.). Obtenido de <https://linube.com/ayuda/articulo/267/que-es-un-virtualhost>
- osi*. (21 de agosto de 2018). Obtenido de <https://www.osi.es/es/actualidad/blog/2018/08/21/que-son-los-ataques-dos-y-ddos>
- Redes Zone*. (s.f.). Obtenido de <https://www.redeszone.net/tutoriales/servidores/ubuntu-server-instalacion-configuracion/>
- todo sobre redes*. (s.f.). Obtenido de <https://sobretodoredes.wordpress.com/redes-cableadas/elementos-de-una-red/interfaces-de-red/>
- TTANDEM*. (s.f.). Obtenido de <https://www.ttandem.com/blog/aumenta-la-seguridad-de-wordpress-con-latch/#:~:text=Latch%20es%20un%20sistema%20de,mientras%20no%20la%20estemos%20utilizando.>
- welivesecurity*. (24 de junio de 2020). Obtenido de <https://www.welivesecurity.com/la-es/2020/06/24/que-es-ataque-fuerza-bruta-como-funciona/>
- welivesegurity*. (s.f.). Obtenido de <https://www.welivesecurity.com/la-es/2021/09/28/que-es-ataque-xss-cross-site-scripting/>
- Wikipedia*. (s.f.). Obtenido de https://es.wikipedia.org/wiki/Mod_Security
- wikipedia*. (25 de septiembre de 2021). Obtenido de https://en.wikipedia.org/wiki/Mod_qos
- wordpress*. (7 de Septiembre de 2016). Obtenido de https://juantrucepei.wordpress.com/2016/09/07/instalacion-y-configuracion-de-modulo-mod_evasive-servidor-web-apache/