Instalación

1. Introducción y Advertencias

Esta aplicación está asociada a una o varias obras de la editorial OxWord, siendo utilizada en los ejemplos y demostraciones prácticas que en ella o ellas aparecen.

Se trata de un programa diseñado expresamente para ser vulnerable, conteniendo un elevado número de fallos deliberadamente introducidos en su implementación y configuración. No debe, por tanto, ser utilizado como referencia ni modelo, ni reutilizarse la totalidad o parte de su código, a la hora de construir software que deba ofrecer unas mínimas garantías a este respecto.

Por esta misma razón, debe también evitarse su instalación en equipos que presten servicio en producción o cuya seguridad no sea completamente irrelevante. Los servidores utilizados para ello sólo deberían ser accesibles desde aquellos equipos que vayan a ser utilizados durante las pruebas. Se recomienda un entorno virtualizado de equipos y redes sin conexión con el exterior.

Si, a pesar de cuanto aquí se dice y siempre, se fuera a instalar la aplicación en una máquina física, no sería necesario realizar los pasos 3 - Creación del Servidor virtualizado y 5 - Instalación de VirtualBox Guest Additions.

En cualquier caso, debe utilizar esta aplicación bajo su única responsabilidad y tomando todas las medidas de seguridad oportunas. El autor de la misma no se hace responsable de las consecuencias derivadas de su instalación y uso.

2. Configuración

En los ejemplos que aparecen en la obra u obras a la que esta aplicación está asociada se usó un servidor web virtualizado mediante VirtualBox con las siguientes características:

Sistema operativo	Kubuntu 16.04.1
Servidor web	Apache 2.4.18 con soporte para HTTPS
Páginas dinámicas	CGI PHP 7.0.8
Base de Datos	MySQL 5.7.15
Gestión de la Base de Datos	PHPMyAdmin

Para todos los productos se utilizó la versión disponible en los repositorios oficiales de Kubuntu en el momento de su instalación.

La descarga e instalación de VirtualBox puede realizarse bien a través de los repositorios y sistemas de instalación de software del sistema operativo de su ordenador o bien descargando el correspondiente paquete de

https://www.virtualbox.org/

3. Creación del Servidor virtualizado

El servidor virtualizado utilizará el sistema operativo Kubuntu, cuya imagen ISO de instalación puede ser descargada desde el sitio web

http://kubuntu.org/

Para crear la correspondiente máquina virtual se puede utilizar el botón “Nueva” del gestor de máquinas virtuales de VirtualBox:

Ilustración 1: Nueva

Aparecerá una ventana en la que se podrá dar nombre a la máquina e indicar su futuro sistema operativo:

Ilustración 2: Nom bre y SO

En los siguientes pasos del asistente se podrá seleccionar el tamaño de memoria (ajústese de acuerdo con las características del equipo anfitrión)...

Ilustración 3: RAM

… y las características del disco:

Ilustración 4: Disco

Ilustración 5: Tipo

Ilustración 6: Dinámico

Debe prestarse especial atención al llegar al tamaño del disco. Los 8 GB que VirtualBox usa por defecto pueden ser insuficientes. En particular, debido a ello, el asistente no permitió pasar de la fase “Preparándose para instalar Kubuntu” durante las pruebas realizadas, siendo preciso ampliarlos:

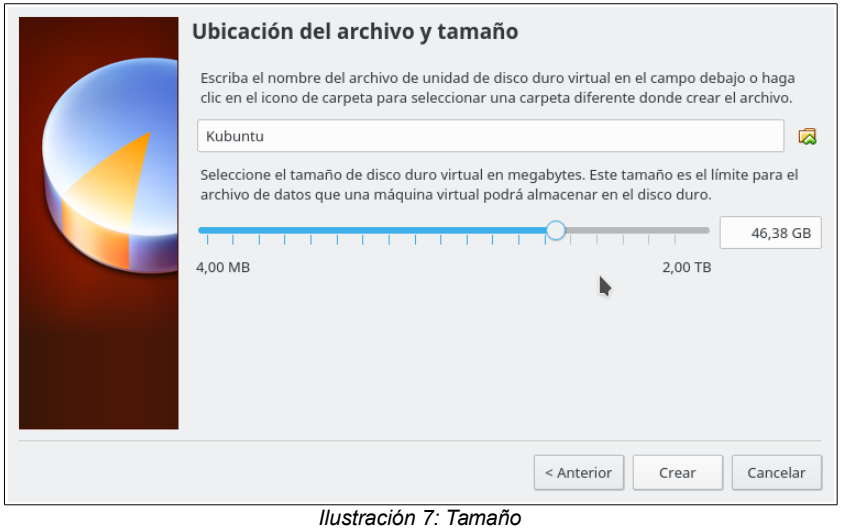

Ilustración 7: Tamaño

. Una vez finalizado el asistente, VirtualBox creará la máquina.

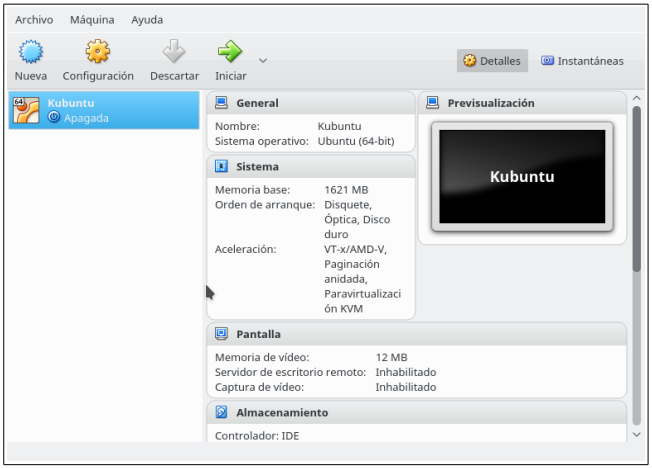

Ilustración 8: Creada

Usando el botón “Configuración” de la parte superior de la ventana se abrirá una ventana con más ajustes. En ella se podrá establecer la posibilidad de compartir el portapapeles y arrastrar ficheros entre host e invitado. Esto puede ser útil durante el proceso de instalación y preparación del servidor web. Una vez deje de ser necesario, se recomienda se deshabilite estas opciones con objeto de aislar el equipo virtualizado de cualquier otro entorno:

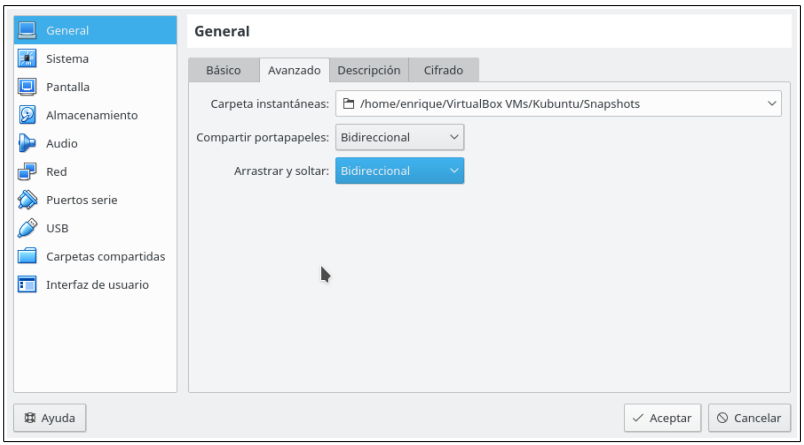

Ilustración 9: Copiar y pegar

También es conveniente asegurarse de que se configura un ratón como dispositivo apuntador…

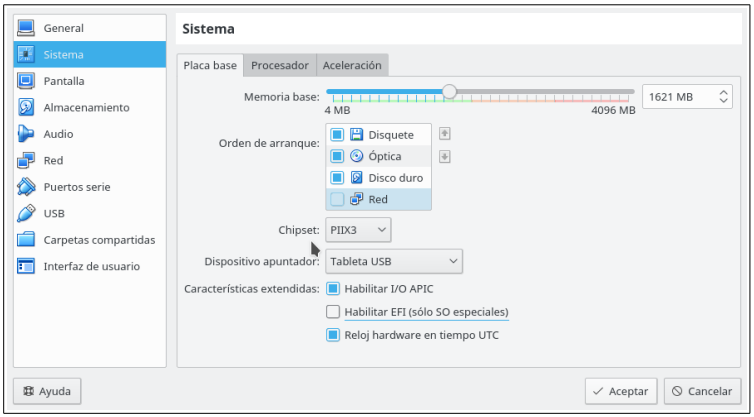

Ilustración 10:

… Y de que se realiza una adecuada selección del uso de procesadores por parte de la máquina virtual:

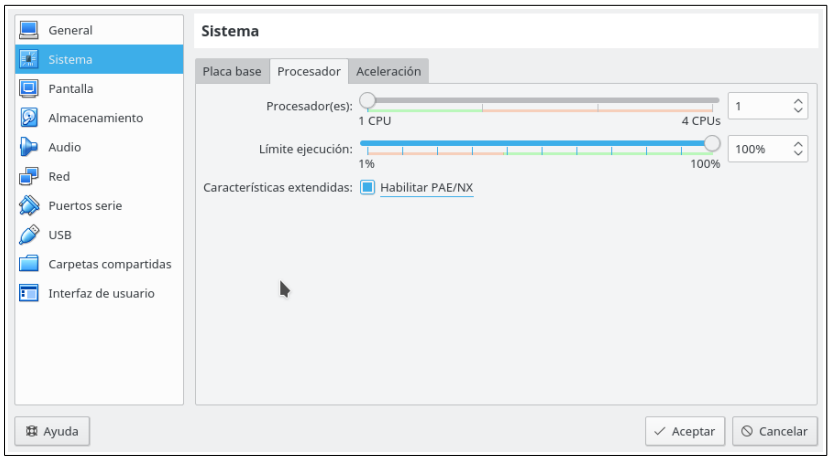

Ilustración 11: CPU

… y de las características de virtualización:

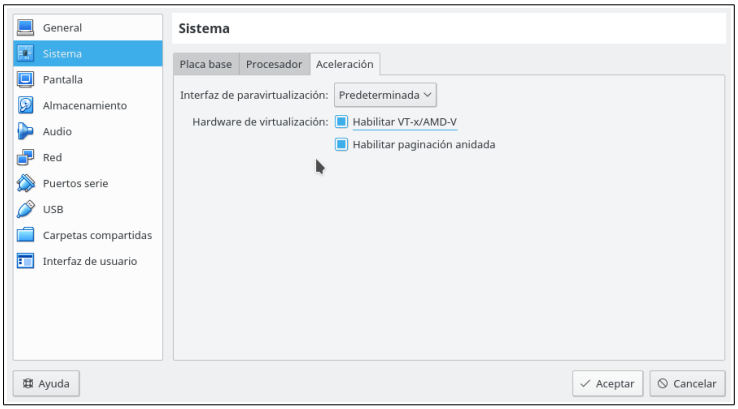

Ilustración 12: Virtualización

Para acabar, se asociará a la unidad lectora de CD-DVD la imagen ISO de instalación de Kubuntu descargada anteriormente:

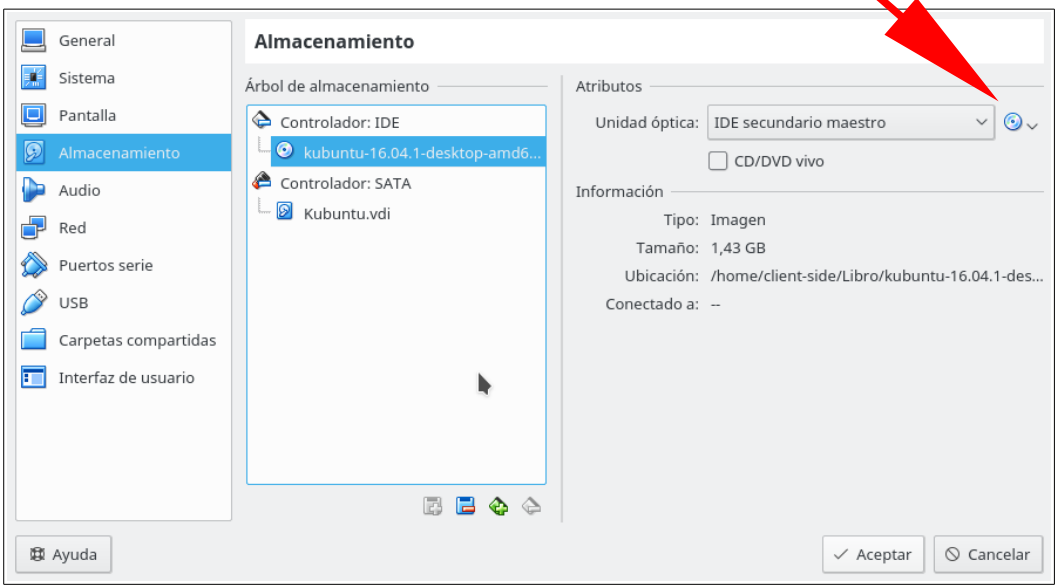

Ilustración 13: Imagen de instalación°

Tras pulsar “Aceptar” se volverá al gestor de máquinas de VirtualBox.

NOTA: El tamaño de la memoria de video asignado por VirtualBox puede ser demasiado pequeño y producir fallos en la interfaz de usuario de la máquina virtual. Si esto supusiera un inconveniente, puede solucionarse incrementando a 56 MB, por ejemplo, la memoria de vídeo en el apartado “Pantalla” de la configuración de la máquina virtual.

4. Instalación del Sistema Operativo en la máquina virtual

Para arrancar la máquina virtual se puede usar el botón “Iniciar” de la parte superior del gestor de máquinas virtuales. Cuando acabe la carga del sistema operativo desde el DVD virtual, en el escritorio de ésta aparecerá un icono que permitirá realizar la instalación.

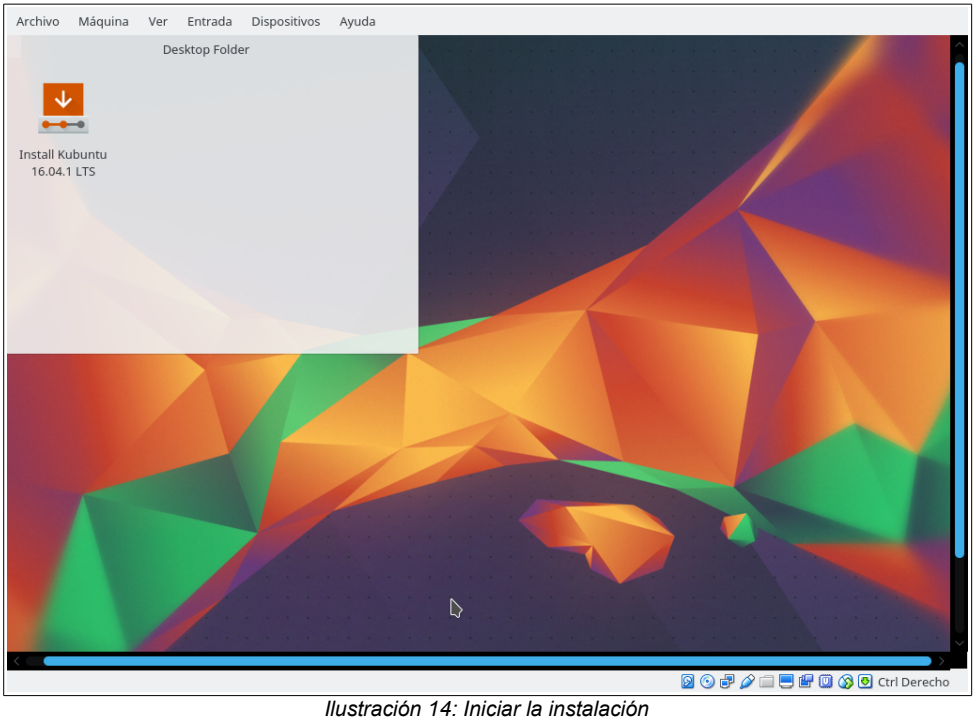

Ilustración 14: Iniciar la instalación

Basta con hacer un clic sobre él para que se inicie el asistente. En su primer paso se preguntará por el idioma a utilizar. Una vez realizado este ajuste, se pedirá permiso al usuario para realizar descargas durante la instalación e instalar software adicional

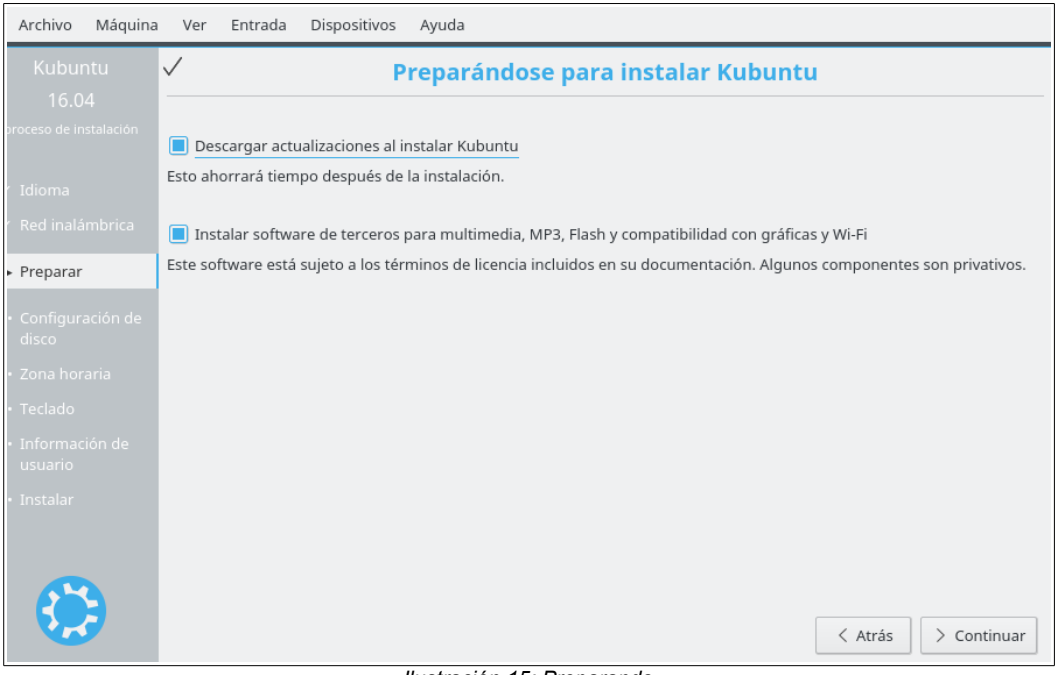

Ilustración 15: Preparando

A partir de ahí se puede ir aceptando las opciones por defecto que ofrece el asistente. Al final, tras pedir un nombre de usuario y una contraseña para el primer usuario del sistema se iniciará el proceso de instalación.

Cuando éste termine, se podrá reiniciar el equipo y comenzar a utilizarlo. Iníciese la sesión con las credenciales introducidas anteriormente y se estará en condiciones de pasar al siguiente apartado.

5. Instalación de VirtualBox Guest Additions

Si se desea poder establecer relaciones entre la máquina virtual y el anfitrión, o si simplemente se desea mejorar la forma en que se gestiona la resolución de pantalla, se deberá instalar las VirtualBox Guest Additions.

Para ello, una vez iniciada la sesión y cargado el entorno de escritorio, se usará la última de las opciones del menú “Dispositivos” de la ventana de la máquina virtual, “Insertar imagen de CD de las “Guest Additions”:

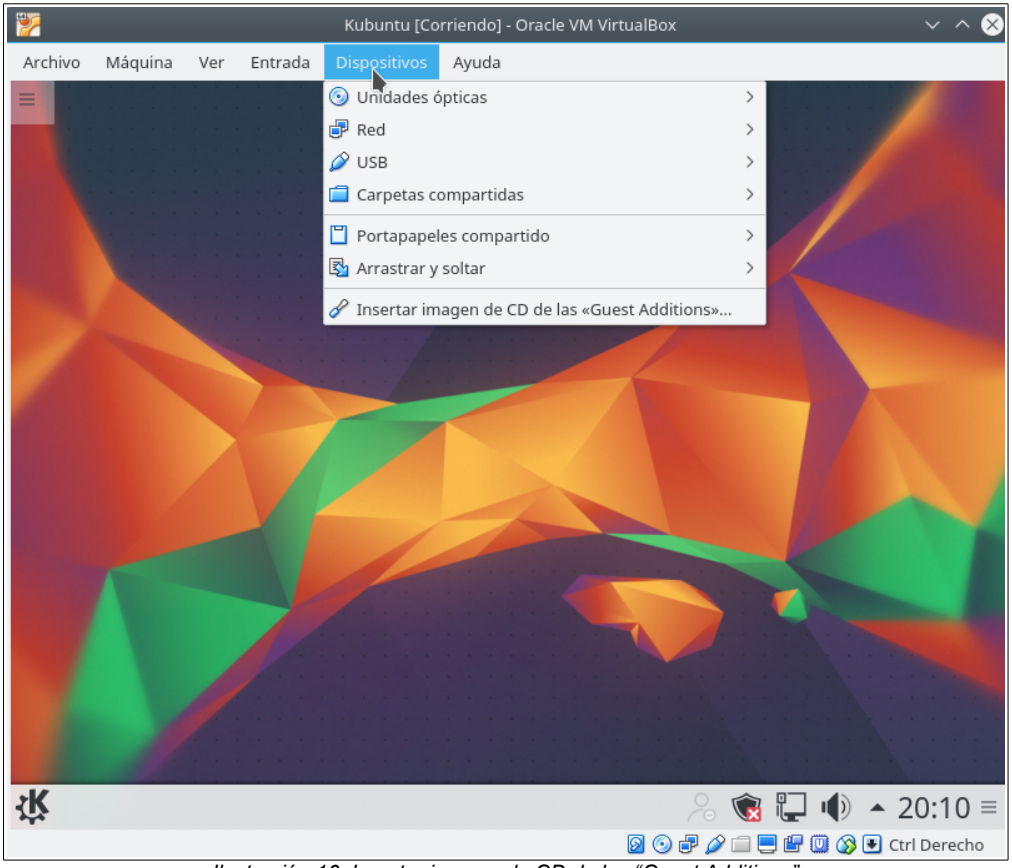

Ilustración 16: Insertar imagen de CD de las “Guest Additions”

Si no lo ha hecho previamente, VirtualBox le indicará que debe descargar antes la imagen. Tras aceptar esta indicación, así como cualquier confirmación posterior, el instalador estará listo para su uso:

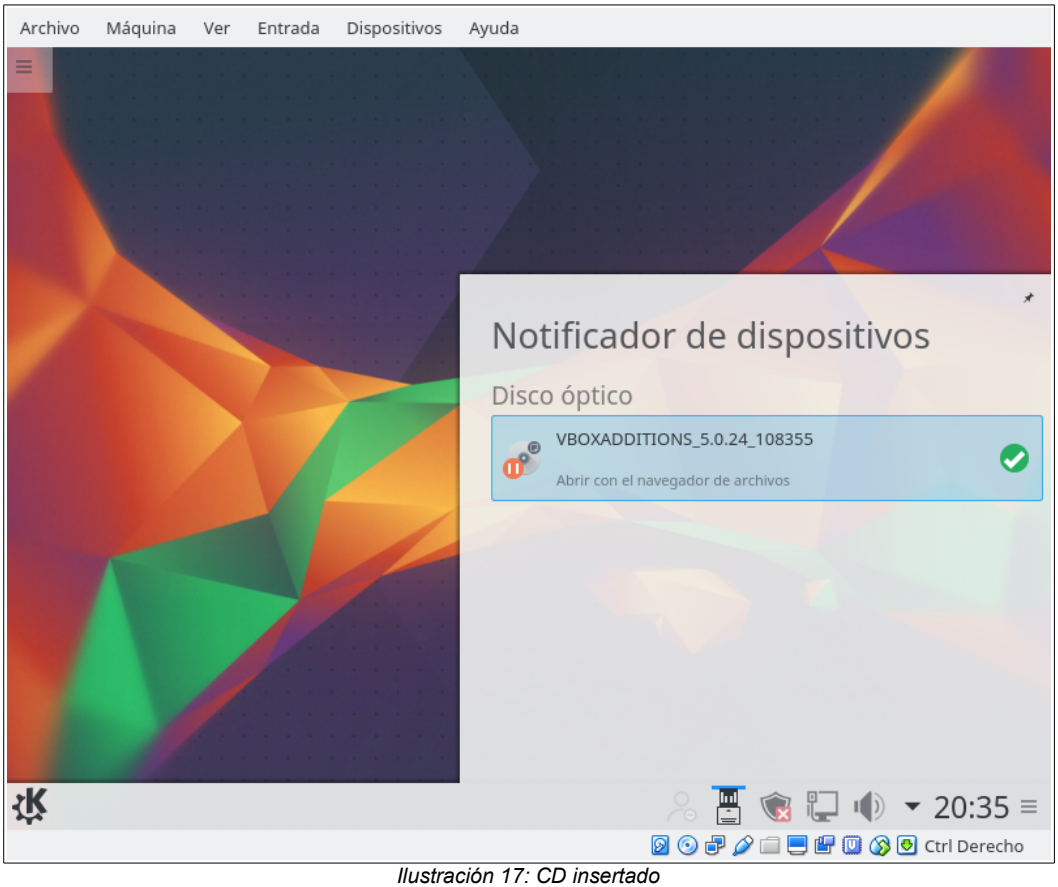

Ilustración 17: CD insertado

Usando la opción “Abrir con el navegador de archivos” se forzará el montaje de la imagen de CD en el sistema de ficheros de la máquina virtual. Después, podrá determinarse su ruta ejecutando en ella el comando

```
mount | grep VBOX
```

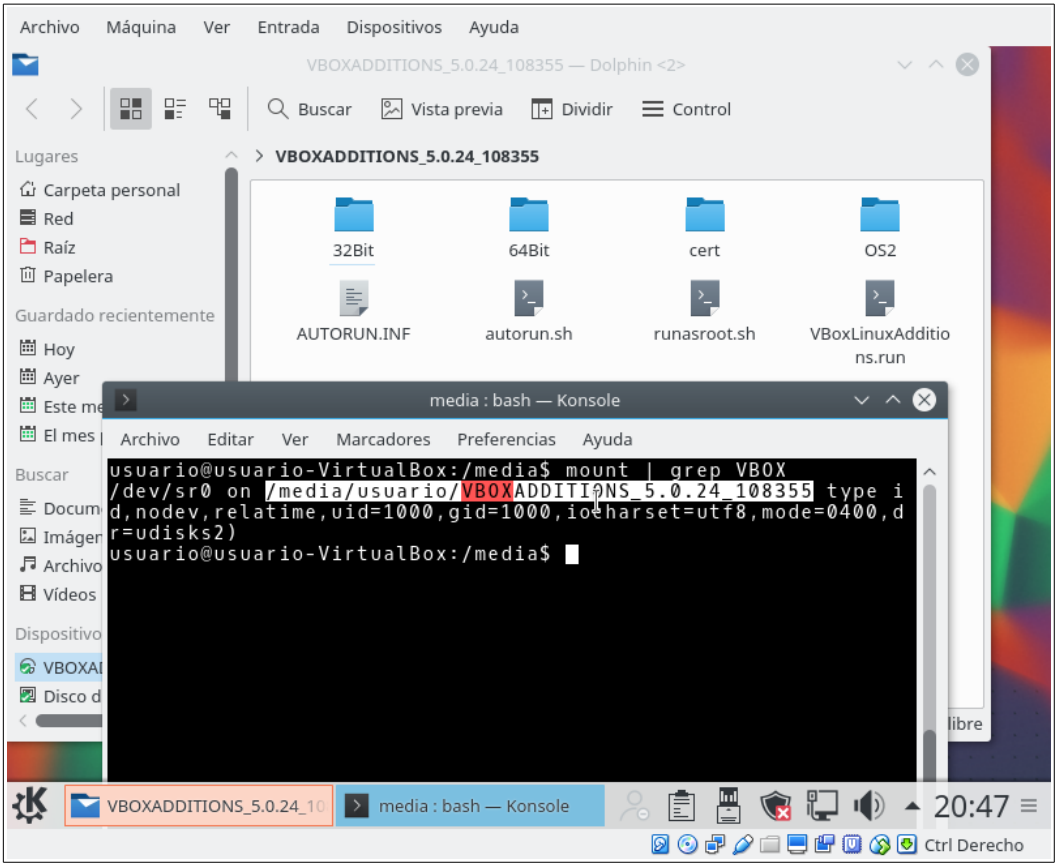

Ilustración 18: ruta

Sólo queda ejecutar el shell script “VBOXLinuxAdditions.run”, ubicado en dicho directorio en modo de administrador. Para la ruta anterior se tendría:

```
cd /media/usuario/VBOXADDITIONS5.0.24_108355

sudo sh VBOXLinuxAdditions.run
```

Tras un rato de trabajo del sistema, será necesario reiniciar la máquina virtual.

■ ■ ■

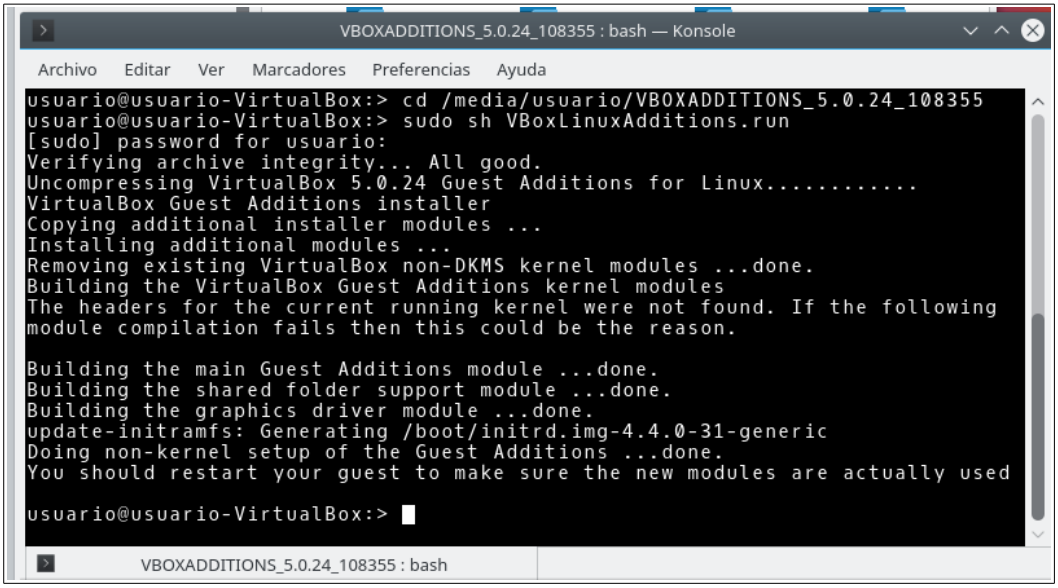

Ilustración 19: Instalación

6. LAMP

Cuando el equipo vuelva a arrancar, y tras iniciar de nuevo sesión en él, se procederá a instalar en él un servidor LAMP (Linux – Apache – MySQL – PHP).

Para ello se deberá abrir un terminal y ejecutar en él la siguiente orden:

```
sudo apt-get install apache2 php mysql-server libapache2-mod-php php-mysql
```

El proceso de instalación comenzará y requerirá poca intervención por parte del usuario. Sólo asignar una contraseña al usuario root de MySQL (no confundir con el root de Linux). Se recomienda que se ponga una contraseña y no se deje en blanco. No sólo por motivos de seguiridad, sino porque esto facilitará posteriormente el uso de PHPMyAdmin

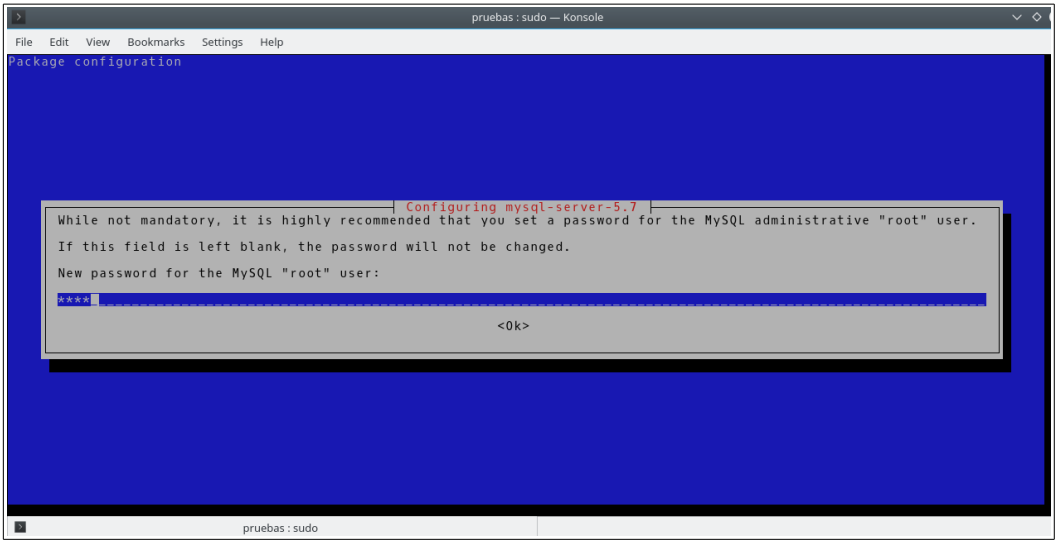

Ilustración 20: Contraseña MySQL

7. HTTPS

Con el servidor web ya operativo, se procederá a habilitar el uso de HTTPS. Para ello, en primer lugar, se activará el módulo SSL de Apache con:

```
sudo a2enmod ssl
```

Después se activará el sitio que trae Apache por defecto para HTTPS. Dicho sitio tiene por nombre “default-ssl” e incluye unos certificados autofirmados que permiten su uso inmediato (aunque el certificado utilizado hará que los navegadores presenten mensajes de aviso):

```
sudo a2ensite default-ssl
```

Para que la nueva configuración tenga efecto hará falta reiniciar el servicio de Apache:

```
sudo service apache2 restart
```

8. CGI

Para acabar la configuración del servidor web, se activará el soporte para CGI de Apache con los siguientes comandos:

```
sudo a2enmod cgi

sudo service apache2 restart
```

9. CURL

La siguiente instrucción añade soporte a PHP para realizar peticiones HTTP usando CURL

```
sudo apt-get install php-curl

sudo service apache2 restart
```

10. PHPMyAdmin

Con objeto de disponer de una interfaz gráfica para gestionar la base de datos se puede instalar el paquete phpmyadmin. La orden para hacerlo es:

```
sudo apt-get install phpmyadmin
```

Durante la configuración de PHPMyAdmin se pedirá al usuario que indique el servidor web a utilizar.

OJO: AUNQUE EL CURSOR APARECE ENCIMA DE "APACHE2", NO HAY NINGUNA OPCIÓN SELECCIONADA. Para seleccionar "Apache2" habrá que pulsar la barra espaciadora. Entonces, la opción aparecerá marcada con un asterisco:

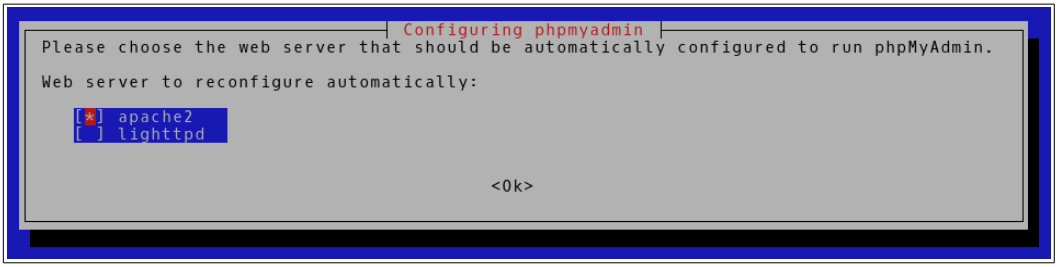

Ilustración 21: Seleccionar Apache2

Tras pulsar INTRO para confirmar la decisión, el proceso seguirá durante unos segundos para después presentar otra pantalla en la que se pregunta si configurar la base de datos para PHPMyAdmin.

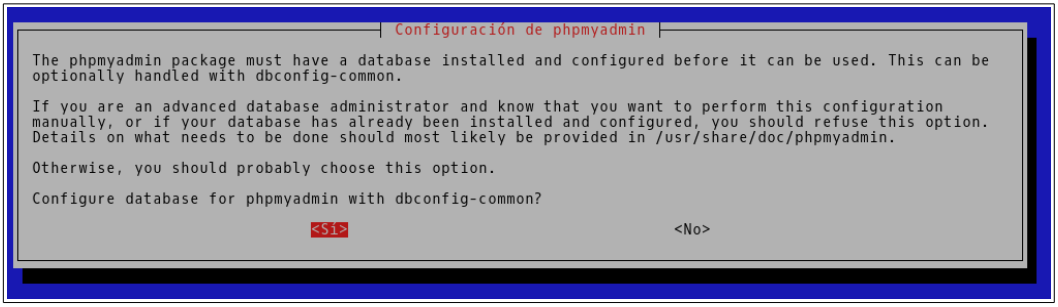

Ilustración 22: Configurar (?)

Pulsando INTRO se aceptará esta operación. Finalmente, cuando se pregunte si se desea indicar una contraseña para registrar PHPMyAdmin en la base de datos, se dejará en blanco el campo y se validará con INTRO para que se genere una clave aleatoria:

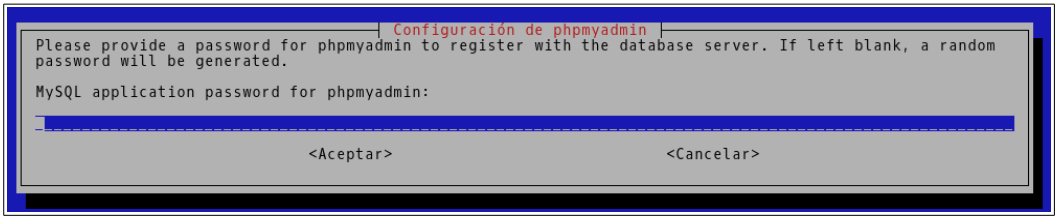

Ilustración 23: Clave

Poco después, la instalación del paquete finalizará. Se podrá comprobar que todo funciona correctamente visitando en la máquina virtual la dirección:

```
https://localhost/phpmyadmin
```

… e iniciando sesión como usuario root y la contraseña elegida al final del apartado 6 - LAMP.

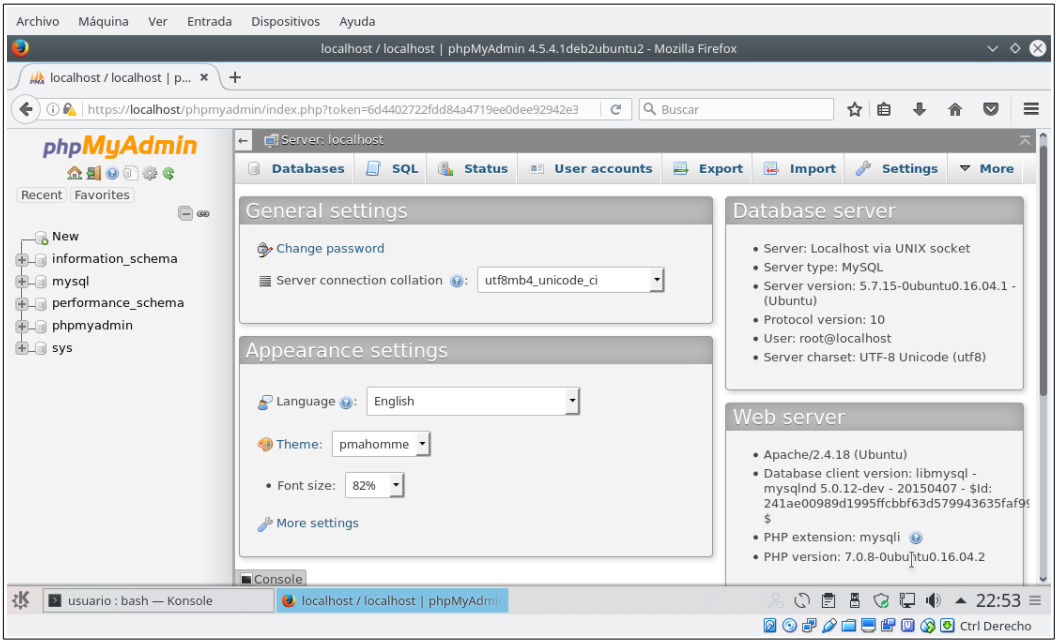

Ilustración 24: PHPMyAdmin

11. Establecer una red entre máquina virtual y anfitrión

Una vez se cuenta con un servidor operativo, se procederá a aislarlo de cualquier entorno que quede fuera del anfitrión que lo hospeda usando una red “Sólo Anfitrión” de VirtualBox.

Para ello se usará la opción “Preferencias” del menú “Archivo del administrador de máquinas virtuales:

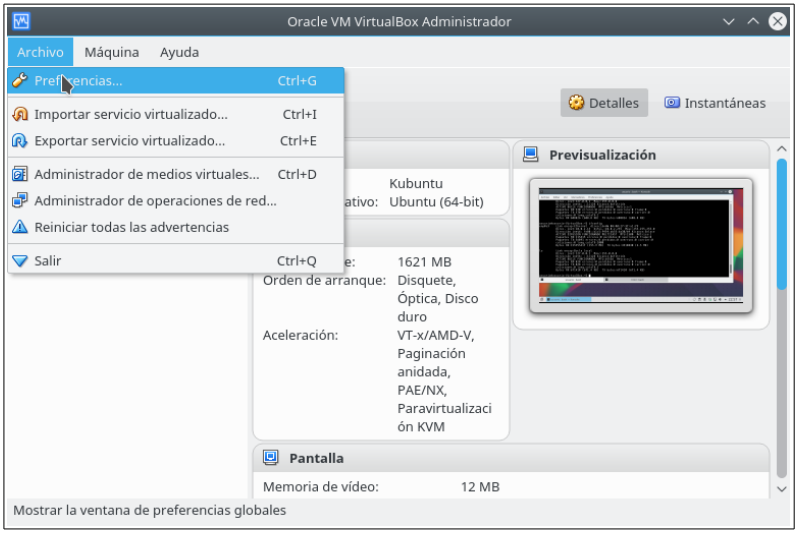

Ilustración 25: Preferencias

Una vez se abra la ventana de ajustes se seleccionará la pestaña “redes sólo-anfitrión” del apartado“Red” y después se hará clic sobre el botón “agregar red”.

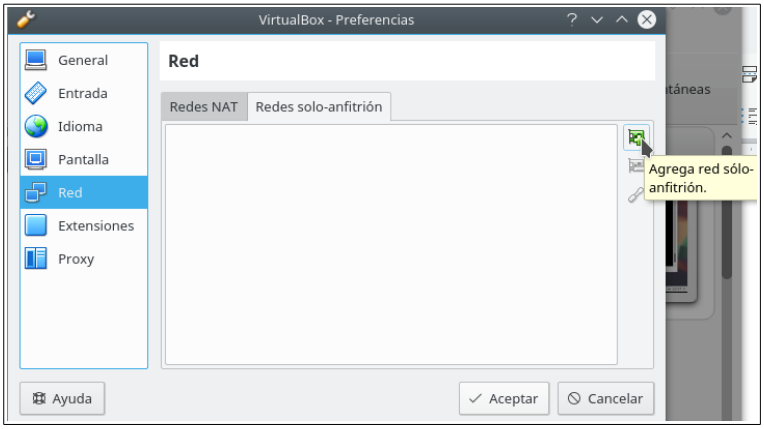

Ilustración 26: Redes sólo-anfitrión

Con ello se habrá creado la red.

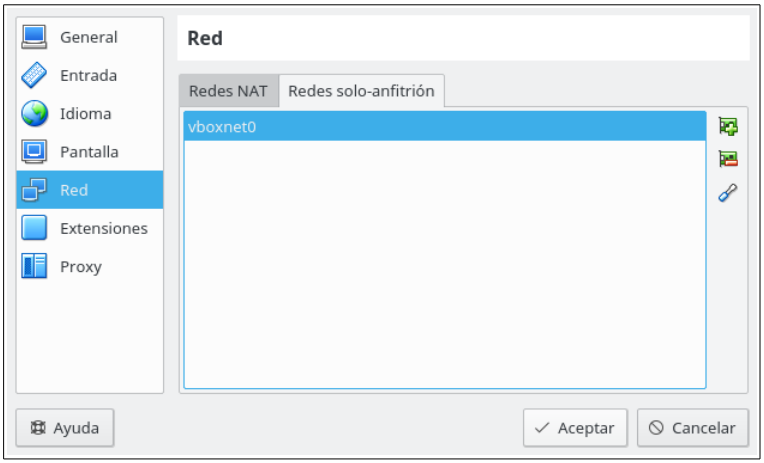

Ilustración 27: Red creada

El anfitrión dispondrá de una nueva interfaz virtual de red cuya configuración puede consultarse y modificarse haciendo doble clic sobre el nombre de la red:

Ilustración 28: Configuración de la red para el anfitrión

OJO: La dirección 192.168.56.1 con máscara 255.255.255.0 se usará como referencia para la configuración de red que más adelante se asignará a la máquina virtual.

Si elige otro direccionamiento de red, tendrá que realizar las correspondientes modificaciones en los pasos posteriores.

Tras cerrar los diálogos abiertos usando sus correspondientes botones “Aceptar”, será necesario asignar la red al servidor web. Para ello se usará el menú “Dispositivos” de la ventana de ejecución de la máquina virtual y las opciones “Red” → “Preferencias de red”.

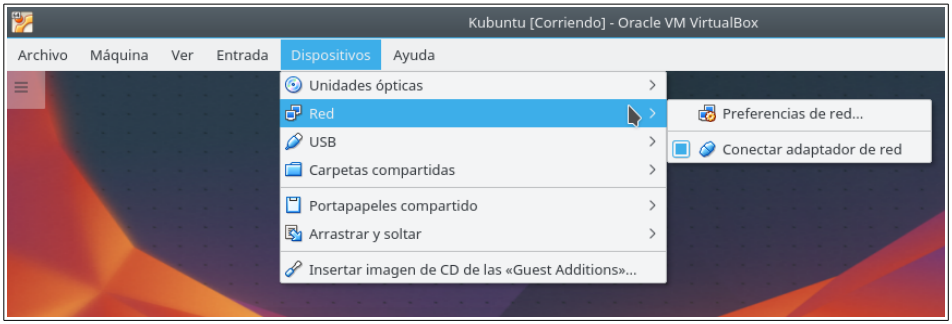

Ilustración 29: Preferencias

En la ventana que se abrirá se deberá seleccionar el valor “Adaptador sólo-anfitrión” en el campo “Conectado a” de las opciones de “Red” y hacer clic en el botón “Aceptar”.

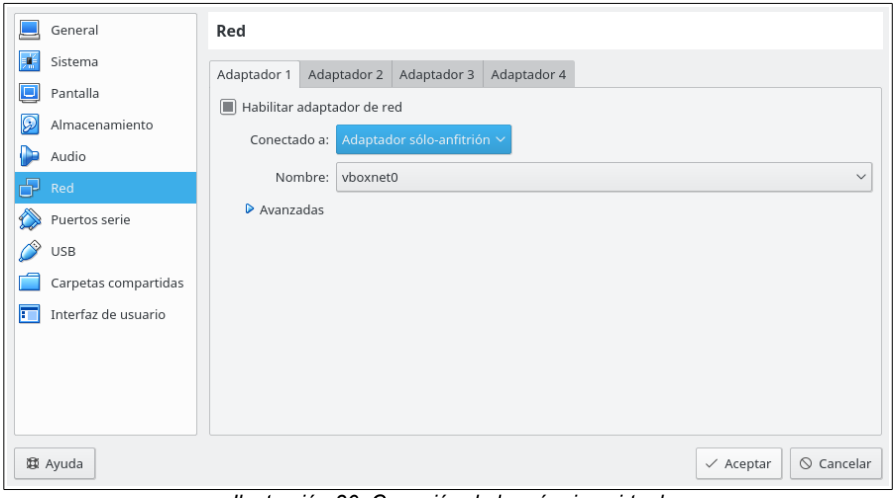

Ilustración 30: Conexión de la máquina virtual

Después se deberá asignar una dirección IP al servidor web. Con un clic del botón secundario del ratón sobre el icono de red del Kubuntu virtualizado se mostrará un menú que permitirá abrir la ventana de configuración de red:

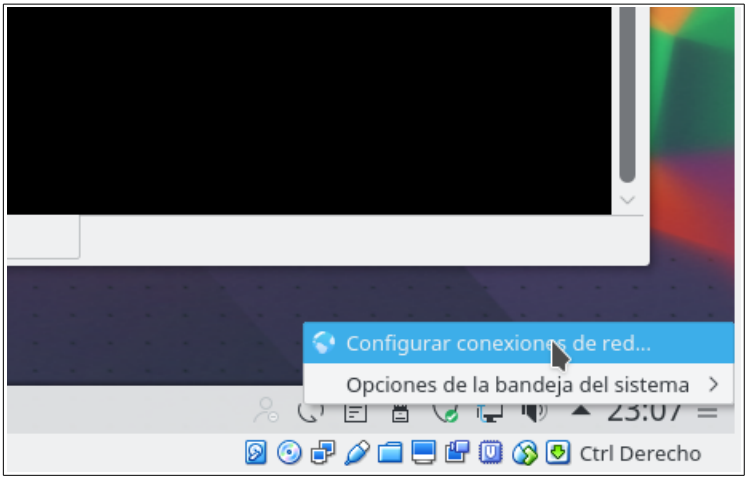

Ilustración 31: Bandeja del sistema de Kubuntu Linux

En ella se podrá editar la conexión de red:

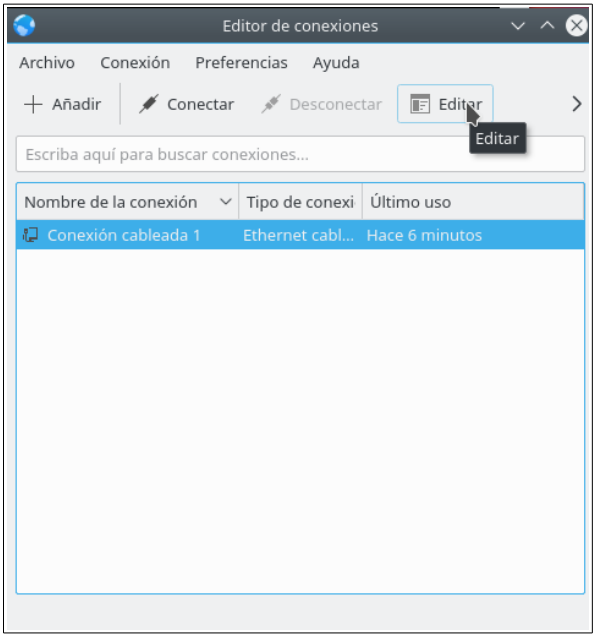

Ilustración 32: Editar

Y, tras indicar que se desea una configuración manual, añadir con el botón “+ Añaadir” una línea de dirección y rellenarla con los datos

Dirección	192.168.56.10
Máscara	255.255.255.0

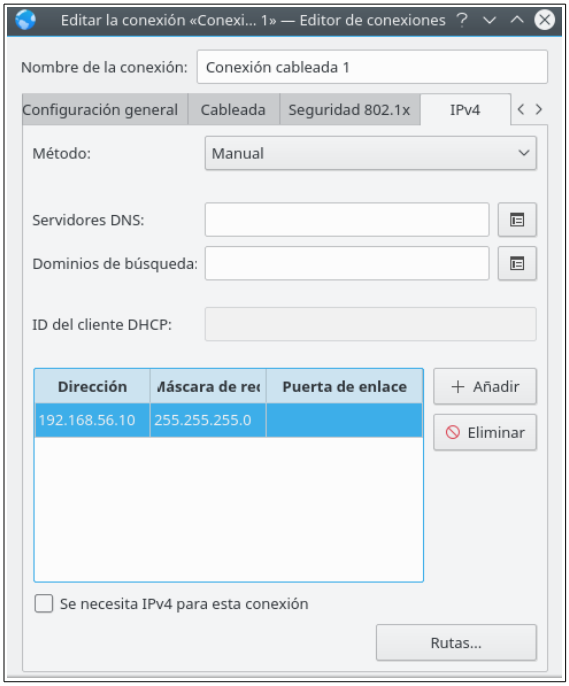

Ilustración 33: Red configurada

Tras cerrar todas las ventanas de ajustes abiertas, anfitrión y máquina virtual compartirán una red privada entre ellos.

12. Copiar los ficheros de la aplicación

Supóngase que ha descargado en la máquina anfitrión el archivo comprimido con los ficheros de la aplicación con el nombre “app.zip”. Para copiarlo a la máquina virtual puede abrir una ventana de comandos y ejecutar en ella las siguientes instrucciones:

```
cd /var/www/html

sudo sh -c "nc -l -p 8000 > app.zip"
```

■ ■ ■

Esto creará un proceso que escuchará en el puerto TCP 8000 y creará un fichero “app.zip” en el directorio raíz del servidor Apache con el contenido que reciba.

En el anfitrión se usará otra ventana para realizar el envío del fichero:

```
nc 192.168.56.10 8000 < app.zip
```

De vuelta a la máquina virtual, se podrá ahora descomprimir el fichero recibido:

```
sudo unzip app.zip
```

También es necesario asignar permisos de ejecución sobre el fichero “aplicacion/descarga_adjunto.cgi”. Quizá haya formas más seguras de hacerlo, pero puesto que se trata de una aplicación deliberadamente vulnerable, se puede salir rápidamente del paso con:

```
cd aplicacion

sudo chmod ugo+x descarga_adjunto.cgi
```

Si se observa el contenido del archivo comprimido se verá que en él se incluye tanto la aplicación vulnerable como los ficheros necesarios para realizar los ataques contra ella. Para eso sirven los directorios “aplicacion” y “ataques” respectivamente. Se podría usar dos servidores web independientes para publicar ambos contenidos pero, con objeto de evitar consumir demasiados recursos, en este caso se configurará Apache para que responda a dos nombres de servidor:

aplicacion.example.com
malicioso.example.net

Dependiendo del nombre de servidor con el que se realice los accesos se proporcionará el contenido de la carpeta “aplicacion” o el de “ataques”. En el primero de estos directorios hay un fichero con la configuración a añadir. Para hacerla efectiva basta con dos comandos:

```
sudo cp zzz-aplicacion.conf /etc/apache2/sites-enabled/
```

```
sudo service apache2 restart
```

13. Configurar el equipo cliente

En el equipo que vaya a ser utilizado como cliente habrá que realizar los ajustes necesarios para que los nombres de equipo “aplicacion.example.com” y “malicioso.example.net” sean resueltos a la dirección de la máquina virtual.

Para ello se puede editar el fichero /etc/hosts. Pero si se desea una solución más flexible se puede también usar el paquete dnsmasq. Para instalarlo basta con ejecutar:

```
sudo apt-get install dnsmasq
```

Después, se podrá configurar el sistema para que cualquier nombre de equipo de los dominios “example.com” y “example.net” sean resueltos a 192.168.56.10 editando el fichero “/etc/dnsmasq.conf” y añadiéndole al final las líneas:

```
address=/example.com/192.168.56.10
address=/example.net/192.168.56.10
address=/apagado.example.edu/192.168.56.111
```

Para que la nueva configuración tenga efecto, habrá que reiniciar el servicio dnsmasq:

```
sudo service dnsmasq restart
```

14. Crear la base de datos

Sólo resta crear la base de datos que da soporte a la aplicación.

Desde el cliente se puede ahora acceder a la página

```
http://aplicacion.example.com/phpmyadmin
```

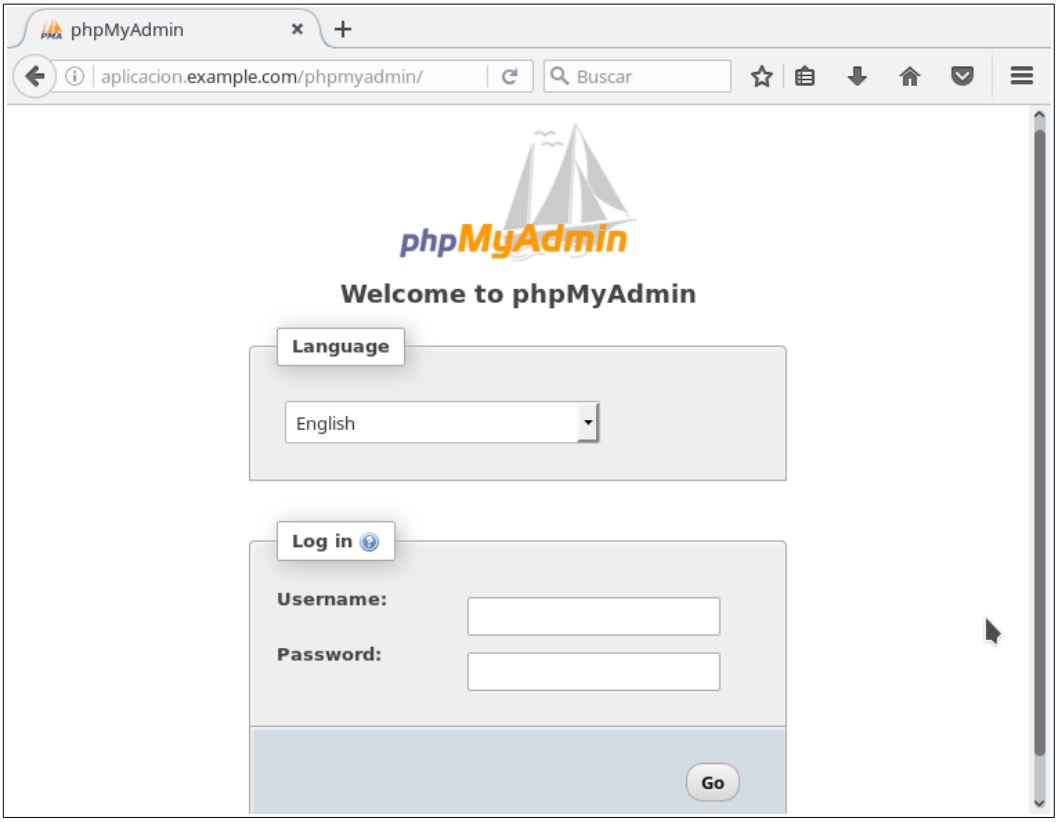

Ilustración 34: PHPMyAdmin

Y, tras iniciar sesión con las credenciales del usuario “root” de MySQL, importar el contenido del fichero “mensajeria.sql” almacenado en la carpeta “aplicacion” del archivo comprimido de instalación.

Nótese que la opción “Importar” (o “Import”) puede quedar oculta si la ventana es demasiado estrecha. En ese caso, se la podrá encontrar dentro del apartado “Más” (o “More”):

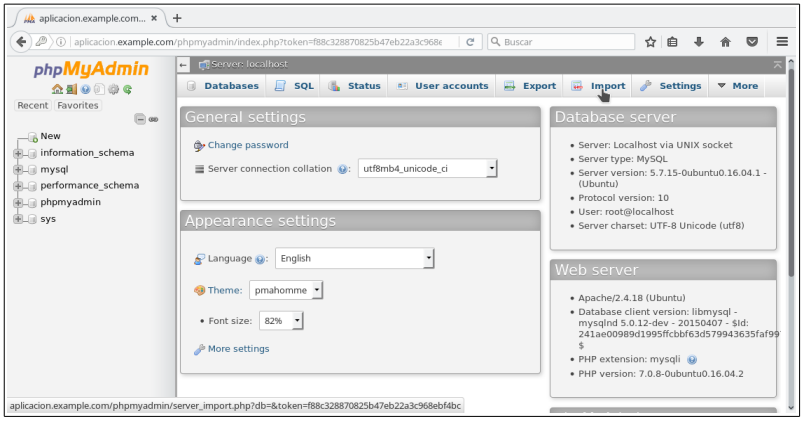

Ilustración 35: Importar

En el formulario que se mostrará sólo será necesario seleccionar el fichero a importar y hacer clic en el botón “Go”:

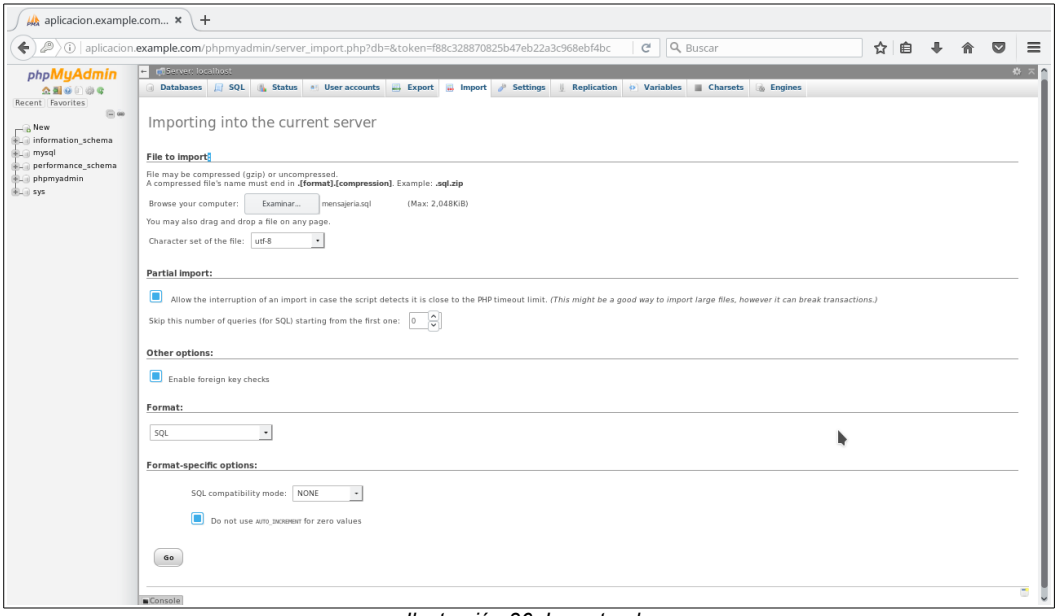

Ilustración 36: Importando

15. Probar

Una vez finalizada la importación, se podrá iniciar sesión en la aplicación. La URL de inicio será:

```
http://aplicacion.example.com
```

Ilustración 37: Aplicación

Y las credenciales que podrá usar son:

Nombre	Clave
admin	passadmin
jefazo	passjefazo
usuario1	12345678
usuario2	passusuario2
operador	operador1

malicioso	passmalicioso
temp	temp

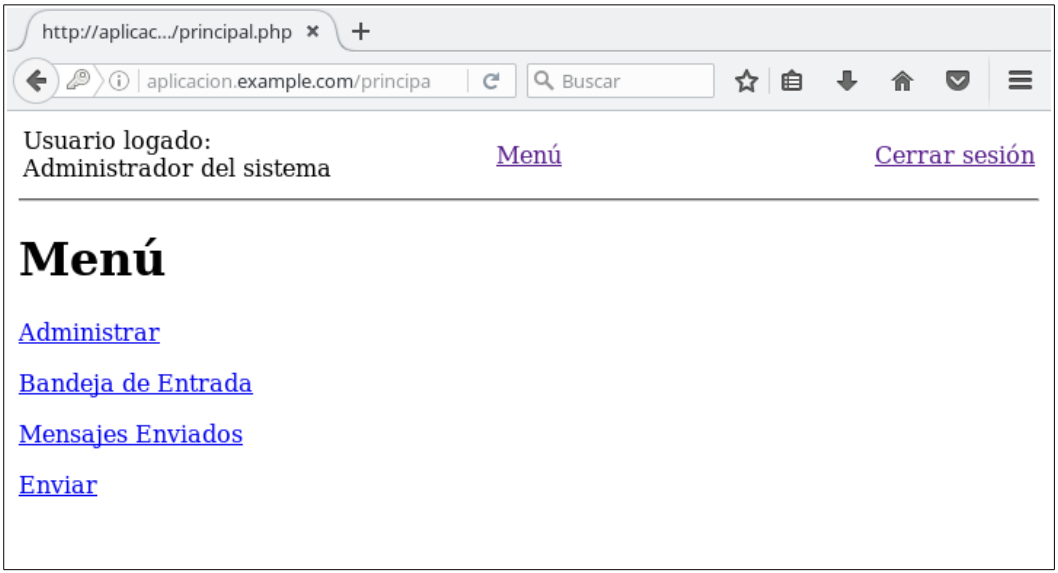

Ilustración 38: Sesión iniciada con admin / passadmin