

Actividad 01. Instalación de Kali Linux

¿Qué es Kali Linux?

Kali Linux es una distribución de Linux desarrollada a partir de Debian que puede utilizarse principalmente para detectar brechas de seguridad en ordenadores o conexiones a Internet, recuperar datos perdidos o analizar contraseñas. El sistema operativo funciona bajo la licencia GNU GPL y, por tanto, es de código abierto. En el futuro, habrá versiones de Kali Linux actualizadas anualmente, que no solo serán mejoradas en términos de contenido, sino que también tendrán nuevos entornos y características. La primera versión de Kali Linux apareció allá por 2013. Los desarrolladores Mati Aharoni y Devon Kearns crearon la distribución para Offensive Security como sucesora a BackTrack. Kali Linux utiliza Xfce como entorno de escritorio.



¿Cuáles son las principales áreas de aplicación de Kali Linux?

Kali Linux tiene más de 600 herramientas de seguridad diferentes y se utiliza principalmente para las pruebas de penetración y la informática forense. La distribución de Linux comprueba las redes y los ordenadores en busca de posibles vulnerabilidades, descifra contraseñas y encriptaciones y evalúa las medidas de seguridad actuales. Kali Linux permite incluso ver o recuperar los datos y archivos borrados o perdidos, siempre que no se hayan sobrescrito. Esto permite a los usuarios comprobar su propia arquitectura de seguridad, detectar y evitar accesos no autorizados o corregir errores de configuración fundamentales que podrían perjudicar su propio sistema o su seguridad.

¿Por qué Kali Linux también es referido como “hacker Linux”?

El término “hacker Linux”, que se utiliza a menudo con respecto a Kali Linux, se debe principalmente a los ámbitos de aplicación mencionados anteriormente. Si hackeas tu propio sistema consigues identificar las vulnerabilidades y cubrir las brechas de seguridad antes de que otros hackers puedan hacer uso de ellas. Sin embargo, también es cierto que las herramientas facilitadas son tan buenas y fiables que, en teoría, también pueden utilizarse para actividades ilegales. Si usas Kali Linux en el ordenador de otra persona puedes explotar esas brechas de seguridad, descifrar contraseñas y sobrecargar y espiar al otro sistema. Eso, por supuesto, está penado por ley.

Kali Linux debe utilizarse únicamente en los equipos propios o en aquellos en los que el usuario haya recibido permiso de acceso explícito. Sin embargo, dado que existe la posibilidad teórica de un uso indebido, la denominación “hacker Linux” puede atribuirse no solo al ethical hacking o al uso en el ordenador propio, sino también a las diversas vías de ataque. Por ejemplo, algunas herramientas

integradas en Kali Linux pueden incumplir los apartados referidos a hackers del art. 197 bis y ter del Código Penal español y podrían llegar a considerarse programas informáticos para el espionaje de datos.

¿Cuáles son los requisitos del sistema operativo?

Instalar Kali Linux es relativamente fácil en comparación con muchas otras distribuciones de Linux. Basta con tener en cuenta los requisitos del sistema. Si quieres instalar Kali Linux en un servidor shell seguro sin interfaz gráfica de usuario, necesitas al menos 128 MB de memoria RAM y 2 GB de almacenamiento en disco. Sin embargo, se recomienda tener al menos 512 MB de memoria RAM. Para instalar Kali Linux con el entorno de escritorio ligero Xfce4 y el kali-linux-default-Metapackage, necesitamos 8 GB de memoria RAM y 20 GB de espacio de almacenamiento para garantizar que el sistema funcione de manera permanente y sin degradación. Sin embargo, técnicamente, 2 GB de memoria RAM son suficientes para la instalación. En cualquier caso, hay que garantizar una conexión a Internet segura y estable.

¿Qué ofrece Kali Linux?

Kali Linux ofrece numerosas herramientas diferentes con las que se puede comprobar y optimizar la seguridad del propio sistema. Entre ellas se encuentra el Social Engineer Toolkit, que contiene varios programas para realizar pruebas de penetración, Metasploit y Aircrack-ng para la identificación de vulnerabilidades en un ordenador o WLAN, y el escáner de seguridad WPSscan para WordPress. Kismet, Nmap o Wireshark, por ejemplo, contribuyen a la seguridad de la red. Se puede comprobar la seguridad de las contraseñas propias con Hashcat y John the Ripper. Estos programas también

pueden utilizarse para crackear cifrados de archivos. Kali Linux ofrece, entre otras cosas, la colección de herramientas The Sleuth Kit para el área de la ciencia forense digital.

¿Cuáles son las ventajas y desventajas de Kali Linux?

Las principales ventajas y desventajas de Kali Linux se encuentran en el enfoque de la distribución de Linux. Si quieres revisar tu ordenador o tu ciberseguridad, Kali Linux te da todas las herramientas necesarias para hacerlo. Difícilmente encontraremos una forma mejor y más fácil de resolver las brechas de seguridad. Su flexibilidad en cuanto a su instalación y su correspondiente finalidad también hablan a favor de la distribución. En combinación con el entorno de escritorio más adecuado, su uso es relativamente intuitivo y se parece en muchos aspectos a los sistemas operativos a los que estamos acostumbrados. Además, Kali Linux cuenta con una gran comunidad, por lo que hay mucha documentación sobre sus diferentes áreas de uso.

Aunque generalmente su uso es relativamente fácil, se necesita mucho tiempo para aprender todas las funciones, sobre todo las más complejas. Kali Linux está diseñado principalmente para usuarios experimentados. También se le achaca repetidamente sus posibilidades de mal uso, lo que puede considerarse una desventaja. Kali Linux se diseñó explícitamente para los propósitos mencionados anteriormente. Sin embargo, si lo que quieres es centrarte en otras acciones que no sean el control de la seguridad, hay otras distribuciones de Linux que son más adecuadas para ti.

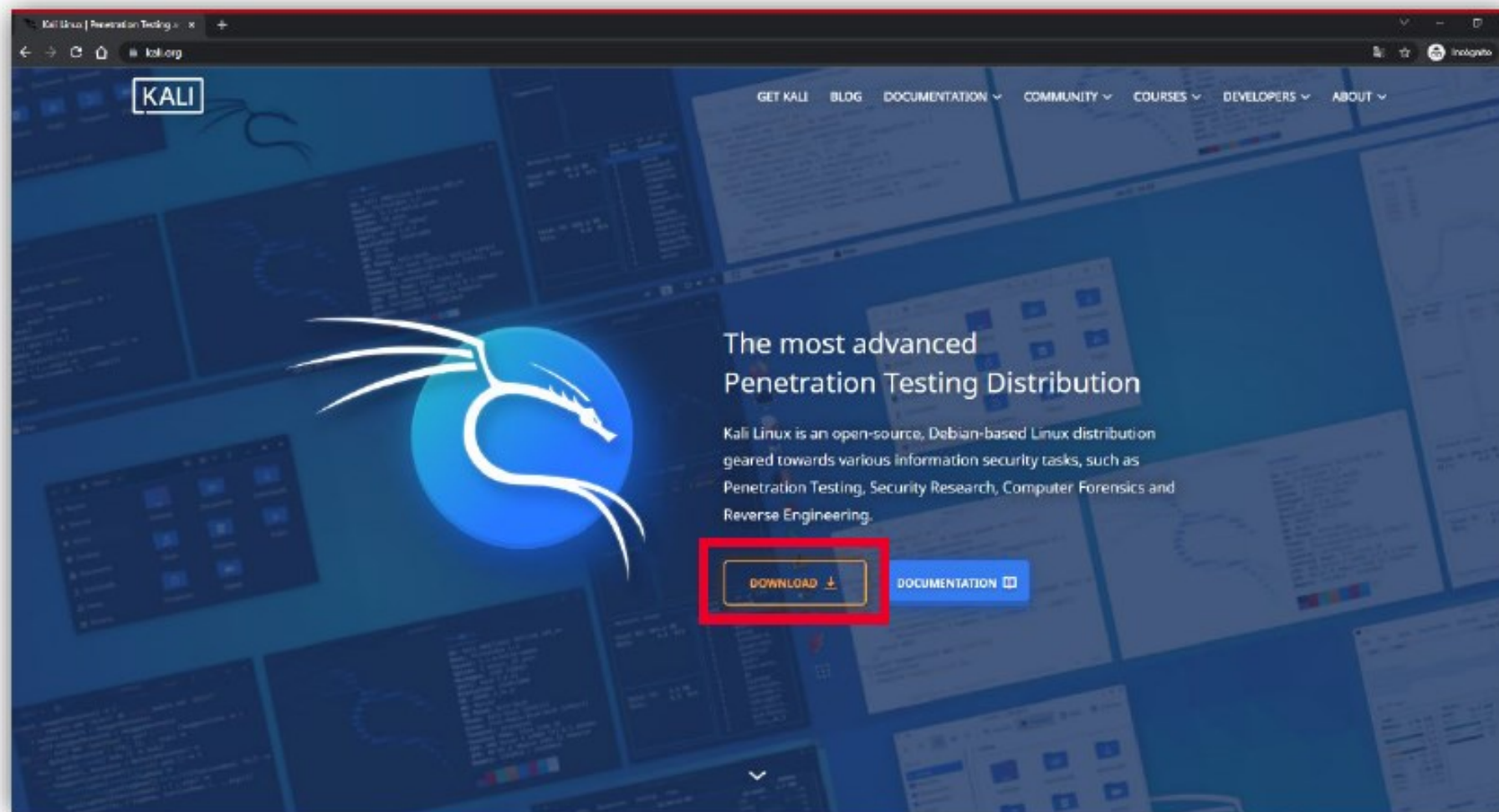
¿Qué alternativas hay a la distribución de Linux?

Si estás buscando una alternativa a Kali Linux que ofrezca funciones similares, BlackArch tiene varios miles de funciones de seguridad y es una buena opción para ti. Arch Linux ha demostrado su eficacia

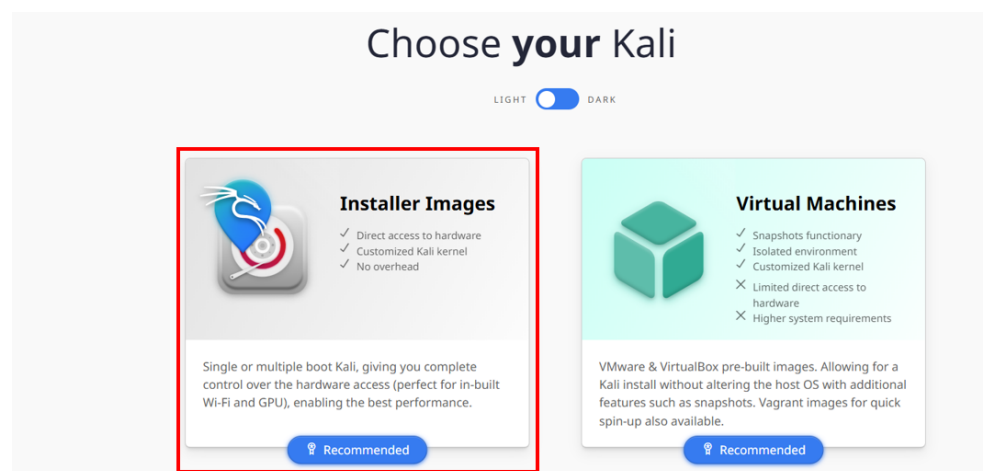
como sistema operativo minimalista con un gran número de opciones de personalización. Manjaro Linux es una alternativa algo más accesible con un frontend gráfico para la gestión de paquetes. Además de distribuciones populares como Ubuntu y Debian, Linux ofrece también distribuciones derivadas, como Linux Mint que es fácil de usar o el ligero sistema Lubuntu. Los dos sucesores de CentOS, Rocky Linux y AlmaLinux, son compatibles con Red Hat Enterprise Linux.

Descarga e instalación de Kali Linux

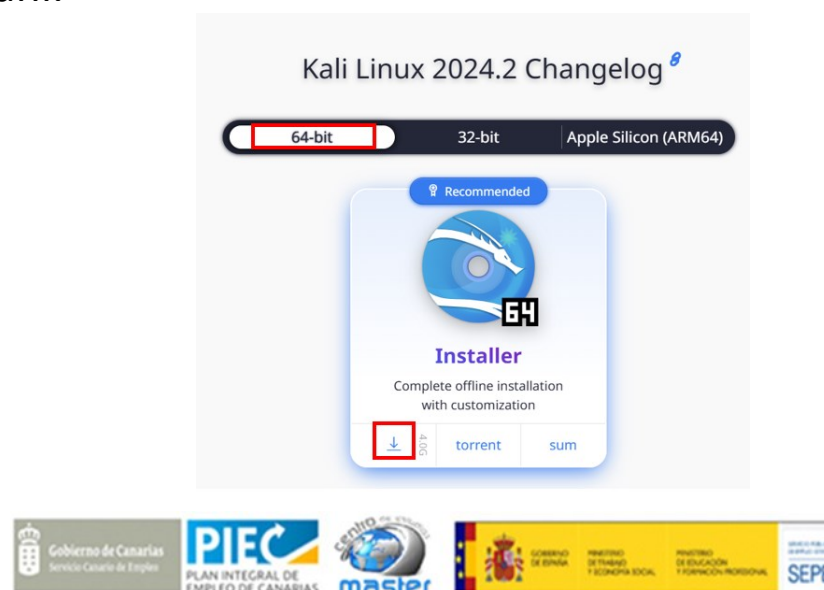
Ahora vas a instalar tu primer sistema operativo en VirtualBox que va a ser Kali Linux. Descarga Kali Linux desde Accede a la página inicio de KaliLinux y haz clic en «Download».



La página te mostrará una lista con todas las plataformas disponibles. En este caso, descarga «Installer Images».



Descarga la imagen de 64-bits. Copia el archivo descargado de la carpeta «Descargas» a la carpeta donde quieras guardar el archivo en tu equipo, por ejemplo, puedes crear una nueva carpeta llamada «Formación» y guardarlo ahí.



Al haber empleado en Kali Linux la opción de Installer Images, crea una máquina en VirtualBox e instala desde la imagen ISO. Sigue los siguientes pasos:

Crear máquina virtual

Nombre y sistema operativo de la máquina virtual

Seleccione un nombre descriptivo y carpeta destino para la nueva máquina virtual. El nombre que seleccione será usado por VirtualBox para identificar esta máquina. Adicionalmente, puede seleccionar una imagen ISO que puede ser usada para instalar el sistema operativo invitado.

Nombre: ✓

Carpeta:

Imagen ISO:

Edición:

Tipo: 64

Versión:

☐ Omitir instalación desatendida

ⓘ No hay imagen ISO seleccionada, el SO invitado será necesario instalarlo manualmente.

Ayuda Modo experto Anterior Siguiente Cancelar

Crear máquina virtual

Hardware

Puede modificar el hardware de la máquina virtual cambiando la cantidad de RAM y número de CPU virtuales. También es posible habilitar EFI.

Memoria base: 4 MB 16384 MB

Procesadores: 1 CPU 16 CPUs

☐ Habilitar EFI (sólo SO especiales)

Ayuda Anterior Siguiente Cancelar

Crear máquina virtual

Disco duro virtual

Si lo desea puede añadir un nuevo disco duro virtual a la nueva máquina. Puede crear un nuevo archivo de disco duro o seleccionar uno existente. De forma alternativa puede crear una máquina virtual sin un disco duro virtual.

☒ Crear un disco duro virtual ahora

Tamaño de disco: 4,00 MB 2,00 TB

☐ Reservar tamaño completo

☐ Usar un archivo de disco duro virtual existente

☐ No añadir un disco duro virtual

Ayuda Anterior Siguiente Cancelar

Crear máquina virtual

Resumen

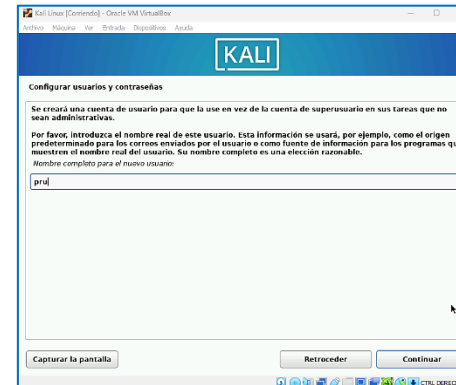
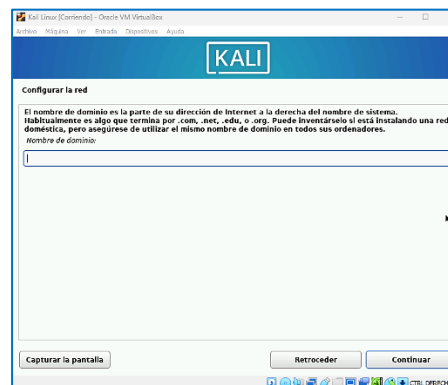
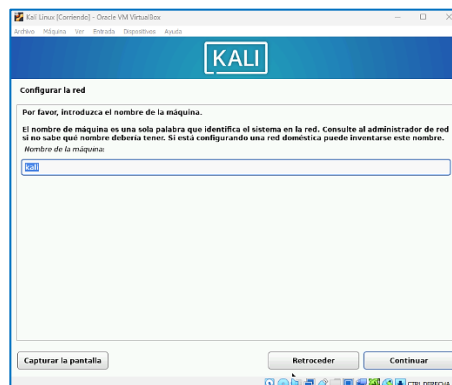
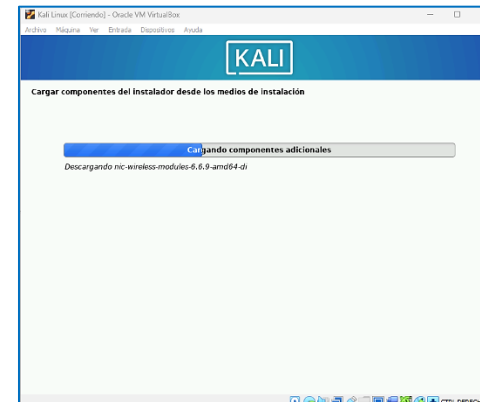
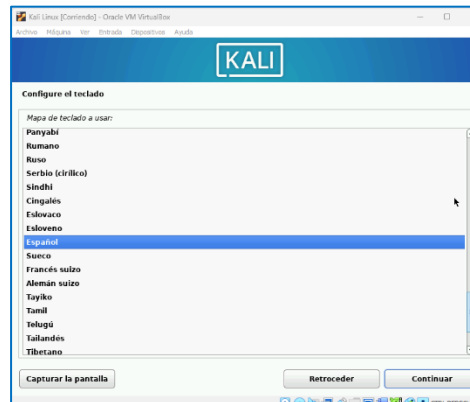
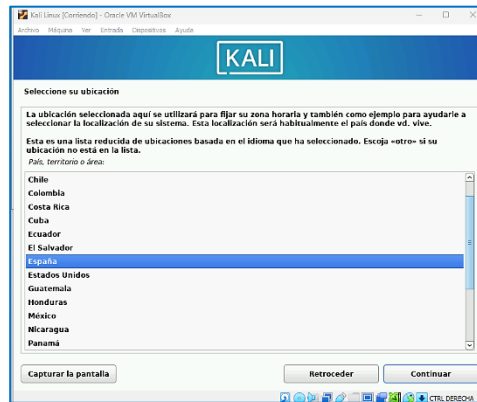
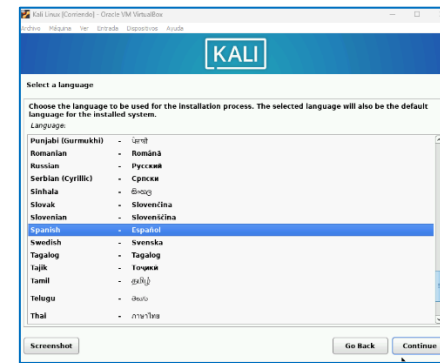
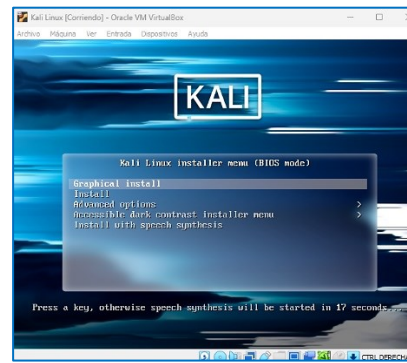
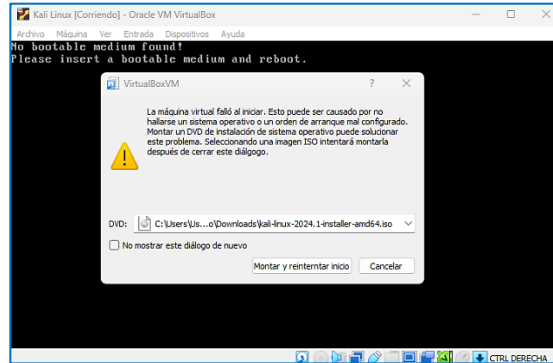
La siguiente tabla resume la configuración que ha elegido para la nueva máquina virtual. Cuando esté conforme con la configuración presione Finalizar para crear la máquina virtual. También puede volver atrás y modificar la configuración.

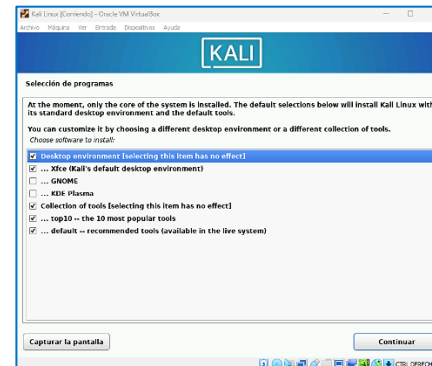
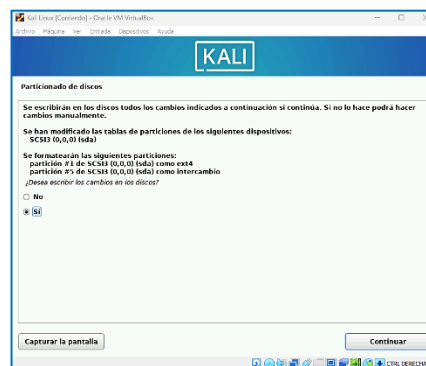
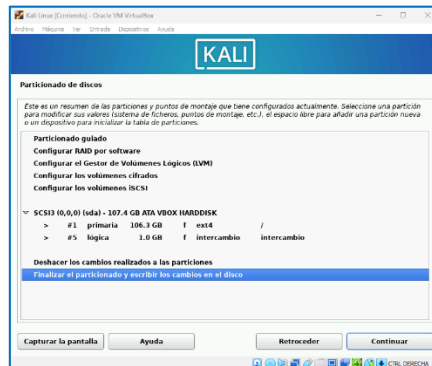
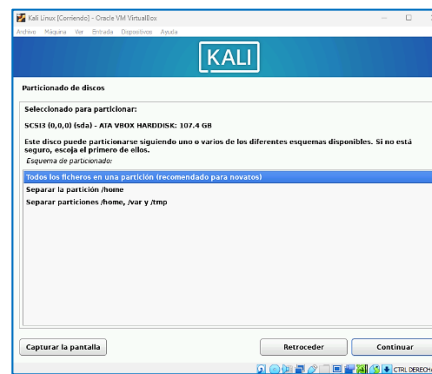
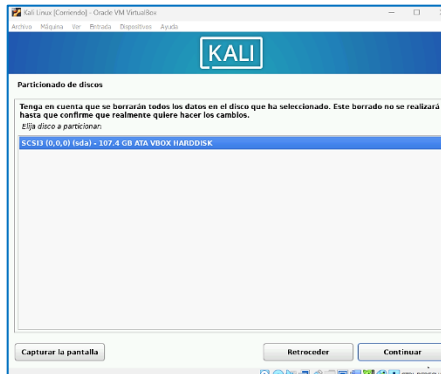
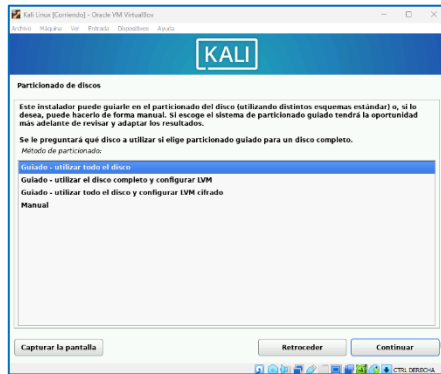
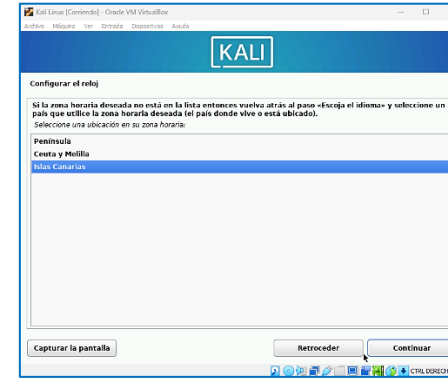
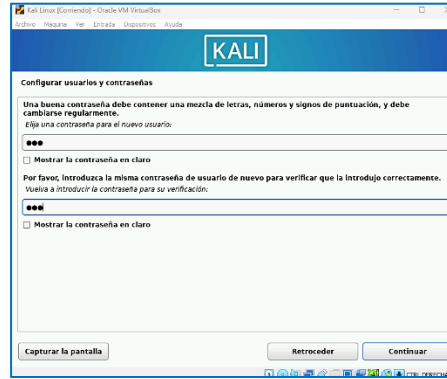
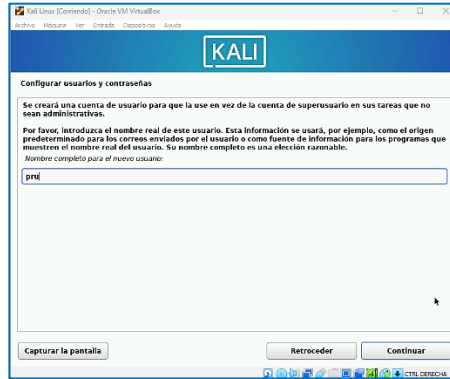
Nombre y tipo de SO de la máquina	
Nombre de máquina	Kali Linux
Carpeta de la máquina	C:\Users\Usuario\VirtualBox VMs\Kali Linux
Imagen ISO	
Tipo de SO invitado	Ubuntu (64-bit)

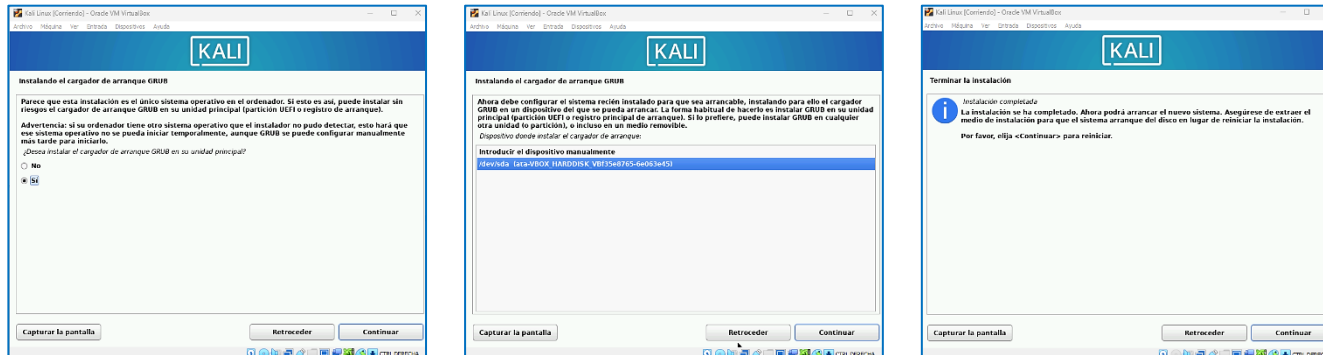
Hardware	
Memoria base	4096
Procesador(es)	4
Habilitar EFI	false

Disco	
Tamaño de disco	100,00 GB
Reservar tamaño completo	false

Ayuda Anterior Terminar Cancelar



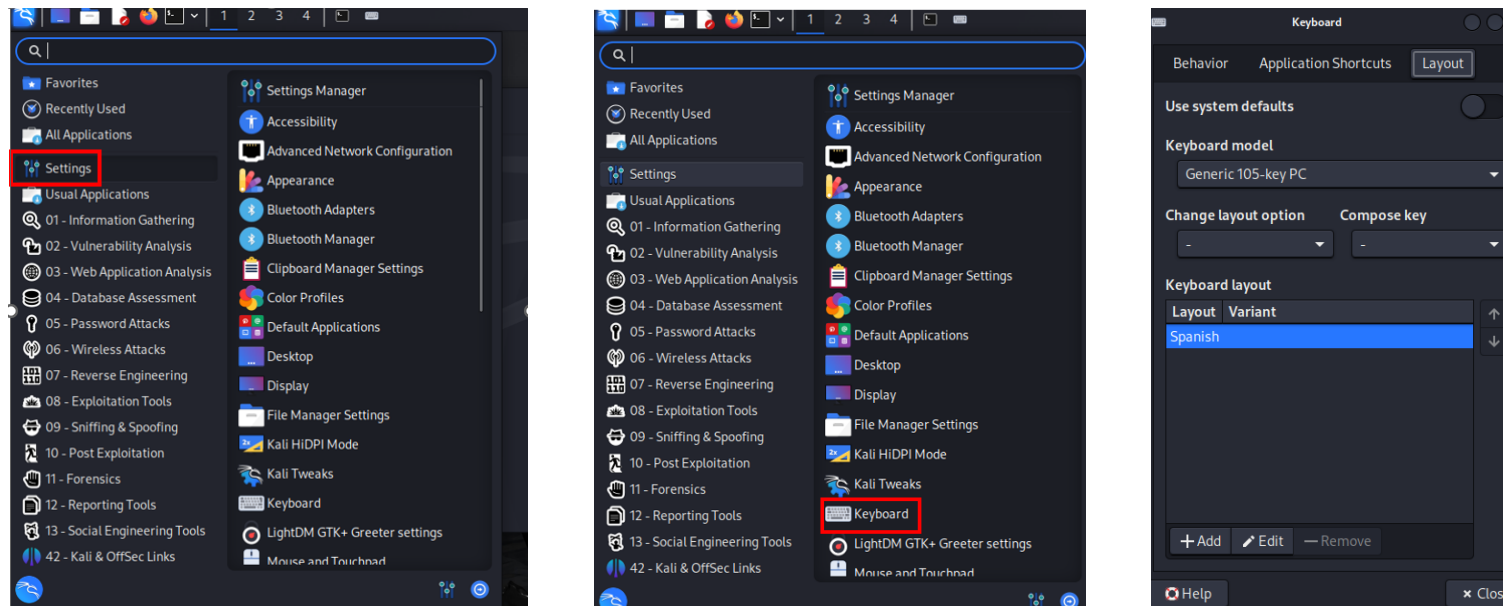




Una vez instalado Kali Linux, vamos a actualizar el sistema:

```
sudo apt update && sudo apt upgrade -y
```

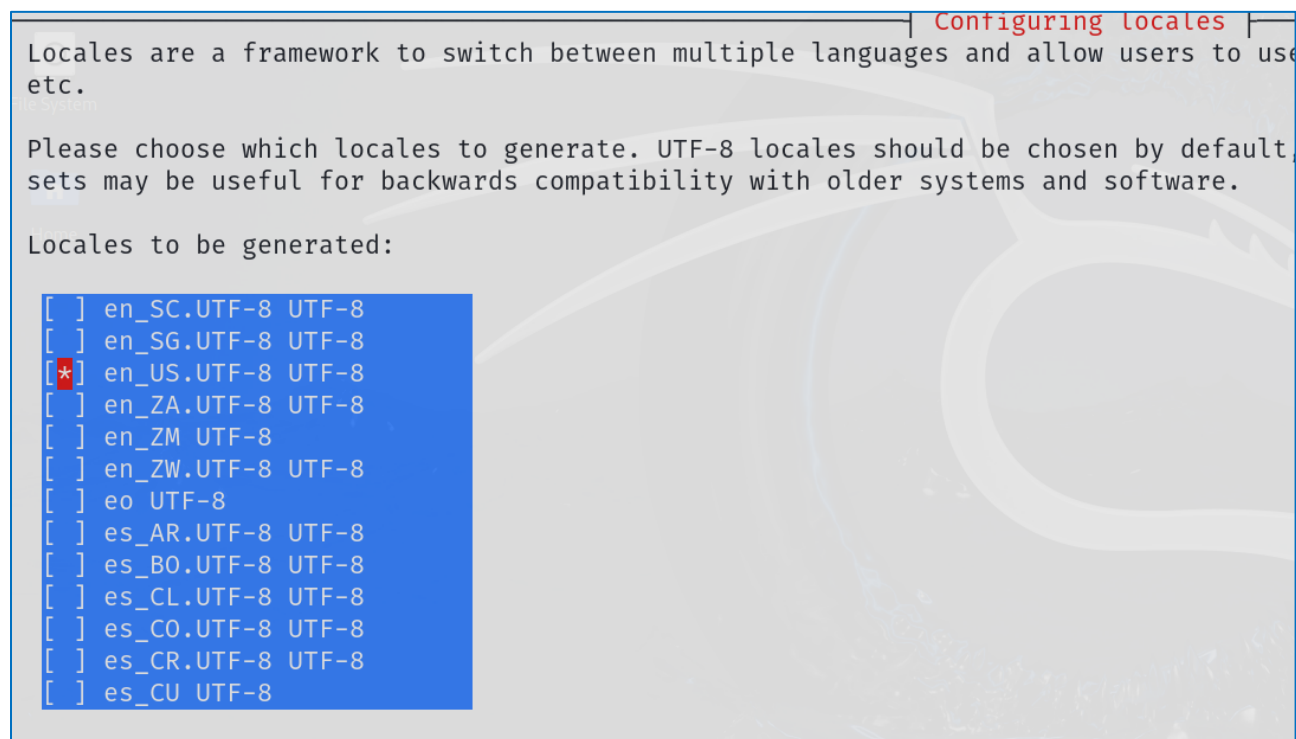
Vamos a cambiar el idioma a español. Para poner el teclado en español, si no estuviera ya:



Para cambiar el idioma en los menús, en la terminal:

```
(kali㉿kali)-[~]  
$ sudo dpkg-reconfigure locales  
[sudo] password for kali: 
```

Desmarcar inglés:



Poner español:

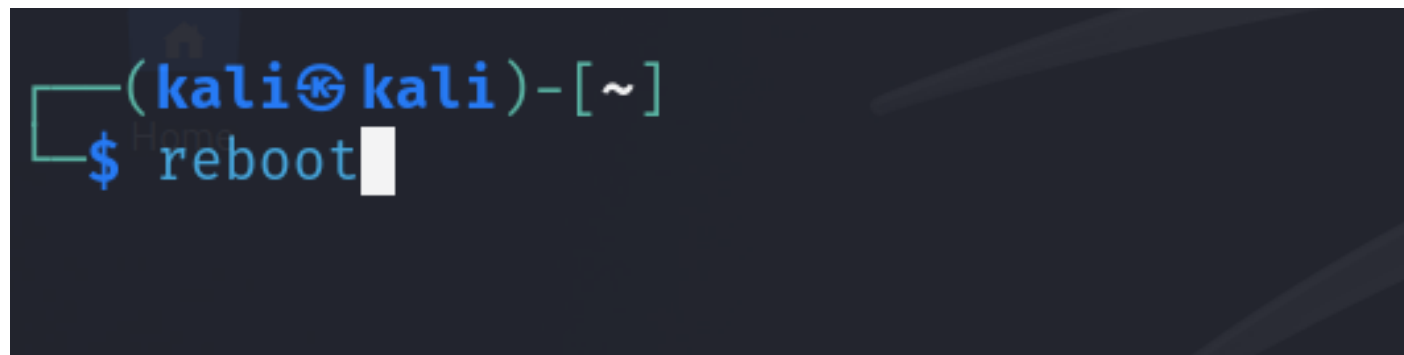
```
Configuring locales
Locales are a framework to switch between multiple languages and allow users to use
etc.

Please choose which locales to generate. UTF-8 locales should be chosen by default
sets may be useful for backwards compatibility with older systems and software.

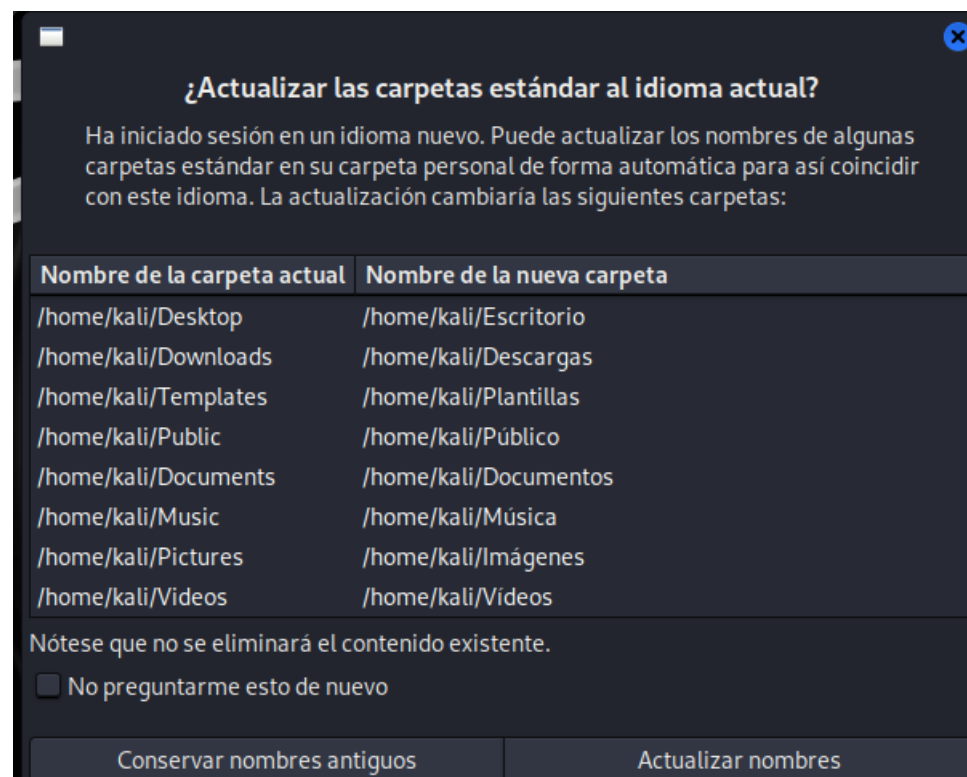
Locales to be generated:

[ ] en_SC.UTF-8 UTF-8
[ ] en_SG.UTF-8 UTF-8
[ ] en_US.UTF-8 UTF-8
[ ] en_ZA.UTF-8 UTF-8
[ ] en_ZM UTF-8
[ ] en_ZW.UTF-8 UTF-8
[ ] eo UTF-8
[ ] es_AR.UTF-8 UTF-8
[ ] es_BO.UTF-8 UTF-8
[ ] es_CL.UTF-8 UTF-8
[ ] es_CO.UTF-8 UTF-8
[ ] es_CR.UTF-8 UTF-8
[ ] es_CU UTF-8
```

Reiniciar



Actualizar nombres:



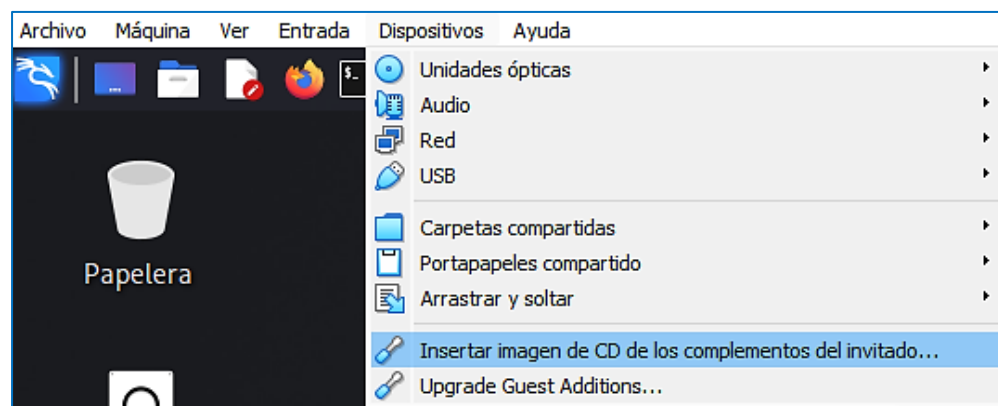
Escribimos los siguientes comandos:

```
sudo apt install linux-headers-$(uname -r) build-essential dkms
```

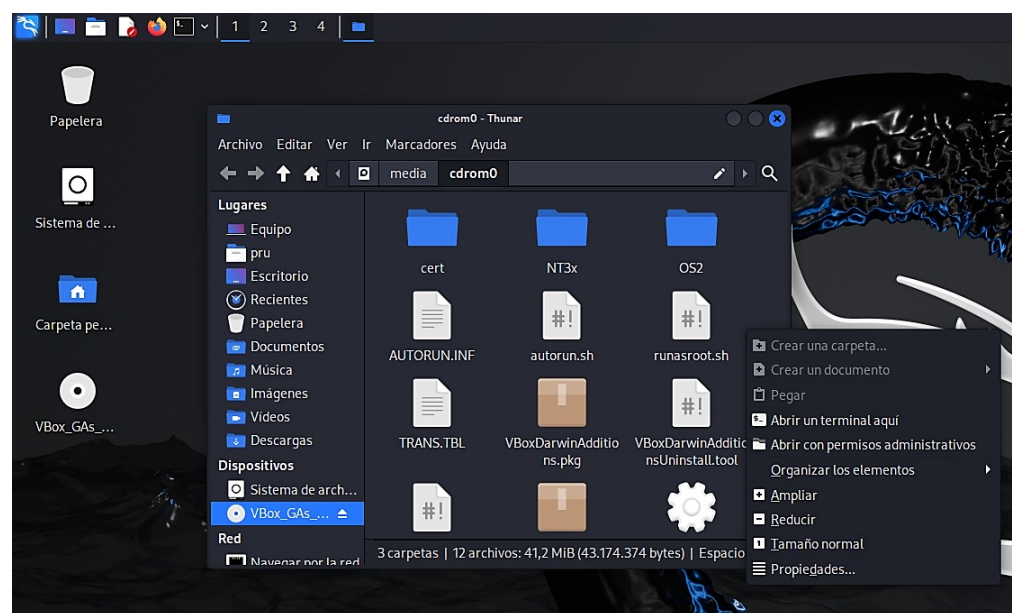
Archivo Acciones Editar Vista Ayuda

```
(pru@kali)-[/media/cdrom0]
$ sudo apt install linux-headers-$(uname -r) build-essential dkms
[sudo] contraseña para pru:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
build-essential ya está en su versión más reciente (12.10).
fijado build-essential como instalado manualmente.
Los paquetes indicados a continuación se instalaron de forma automática y ya no son necesarios.
 libabsl20220623 libadwaita-1-0 libaio1 libappstream5 libatk-adaptor libboost-dev libboost1.83-dev libgphoto2-l10n
 libnsl-dev libopenblas-dev libopenblas-pthread-dev libopenblas0 libpthread-stubs0-dev libpython3-all-dev libpython3.12
 libpython3.12-dev libre2-10 libstemmer0d libtirpc-dev libunibreak5 libxmlb2 libxsimd-dev python3-all-dev python3-anyjson
 python3-beniget python3-diskcache python3-gast python3-mistune0 python3-pendulum python3-pyatspi python3-pypdf2
 python3-pyrsistent python3-pythran python3-pytzdata python3.12-dev xtl-dev zenity zenity-common
Utilice «sudo apt autoremove» para eliminarlos.
Se instalarán los siguientes paquetes adicionales:
 libdw1t64 libelf1t64 libssl3t64 linux-headers-6.8.11-common linux-kbuild-6.8.11 openssl
Paquetes sugeridos:
 menu
Los siguientes paquetes se ELIMINARÁN:
 libdw1 libelf1 libssl3
Se instalarán los siguientes paquetes NUEVOS:
 dkms libdw1t64 libelf1t64 libssl3t64 linux-headers-6.8.11-amd64 linux-headers-6.8.11-common linux-kbuild-6.8.11
Se actualizarán los siguientes paquetes:
 openssl
1 actualizados, 7 nuevos se instalarán, 3 para eliminar y 779 no actualizados.
Se necesita descargar 17,4 MB de archivos.
Se utilizarán 70,3 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n]
```


Vamos a añadir las Guest Additions para poder comunicar la máquina anfitrión con la máquina virtual. En primer lugar, *insertamos la imagen de CD de los complementos del invitado...*



Aparece en el escritorio la unidad de CD, abrimos la ventana y abrimos la terminal en el CD:



```
sudo sh ./VBoxLinuxAdditions.run
```

```
Archivo Acciones Editar Vista Ayuda

(pru@kali)-[/media/cdrom0]
$ sudo sh ./VBoxLinuxAdditions.run
Verifying archive integrity... 100% MD5 checksums are OK. All good.
Uncompressing VirtualBox 7.0.8 Guest Additions for Linux 100%
VirtualBox Guest Additions installer
This system appears to have a version of the VirtualBox Guest Additions
already installed. If it is part of the operating system and kept up-to-date,
there is most likely no need to replace it. If it is not up-to-date, you
should get a notification when you start the system. If you wish to replace
it with this version, please do not continue with this installation now, but
instead remove the current version first, following the instructions for the
operating system.

If your system simply has the remains of a version of the Additions you could
not remove you should probably continue now, and these will be removed during
installation.

Do you wish to continue? [yes or no]
yes
```

reboot

Se pide:

1. Una vez finalizado, sube a la plataforma un documento con capturas de pantalla, que muestren los pasos realizados.