UNIVERSIDAD NACIONAL DE LA MATANZA

Departamento de Ingeniería e Investigaciones Tecnológicas

TP
Practica01 Kali 2017.1

Jefe de Cátedra: *Mg. Jorge Eterovic*

Profesor Ayudante: *Martín Zeballos*

TP 1 BACKTRACK/Kali

Instalar maquina virtual de Kali 2017.1 en VirtualBox

El objetivo de esta práctica es entender que se trata la distribución Kali e instalar una virtual machine desde una imagen ISO. También hay una pequeña práctica para familiarizarse con comandos básicos de Linux.

Diferencias entre Kali Linux y Debian

Kali Linux está orientado a pruebas de penetración profesional y auditorías de seguridad. Como tal, varios cambios han sido implementados en Kali Linux para que reflejen estas necesidades:

- Un solo usuario, acceso root por diseño: Debido a la naturaleza de las auditorías de seguridad, Kali linux está diseñado para ser usado en un escenario “de un solo usuario, root“.
- Servicio de redes deshabilitado en forma predeterminada: Kali Linux contiene ganchos sysvinit los cuales deshabilitan los servicios de redes por defecto. Estos ganchos nos permiten instalar varios servicios en Kali Linux, mientras aseguran que nuestra distribución permanezca segura en forma predeterminada, no importando que paquetes estén instalados. Adicionalmente los servicios tales como Bluetooth son también puestos en lista negra por defecto.
- kernel de linux modificado: Kali Linux usa un kernel, parchado para la inyección wireless.

Si estas buscando una distribución de Linux para aprender las bases y tener un buen punto de partida, Kali Linux no es la distribución ideal para ti. Deberías comenzar con Ubuntu o Debian en su lugar.

¿Qué es Kali Linux?

Características de Kali Linux

Kali Linux es una distribución de Linux avanzada para pruebas de penetración y auditorías de seguridad.

Kali es una completa re-construcción de BackTrack Linux desde la base hacia arriba, y se adhiere completamente a los estándares de desarrollo de Debian. Toda la nueva infraestructura ha sido puesta en el lugar, todas las herramientas fueron revisadas y fueron embaladas, y hemos cambiado a Git para nuestro VCS.

- **Más de 300 herramientas de pruebas de penetración:** Después de revisar todas las herramientas que se incluyen en BackTrack, hemos eliminado una gran cantidad de herramientas que, o bien no funcionaban o tenían otras herramientas disponibles que proporcionan una funcionalidad similar.

- **Gratis y siempre lo será:** Kali Linux, al igual que su predecesor, es completamente gratis y siempre lo será. Nunca, jamás, tendrás que pagar por Kali Linux.

- **Git – árbol de código abierto:** Somos partidarios enormes de software de código abierto y nuestro árbol de desarrollo está disponible para todos y todas las fuentes están disponibles para aquellos que desean modificar y reconstruir paquetes.

- **Obediente a FHS:** Kali ha sido desarrollado para cumplir con el Estándar de jerarquía del sistema de ficheros, permitiendo que todos los usuarios de Linux puedan localizar fácilmente archivos binarios, archivos de soporte, bibliotecas, etc.

- **Amplio apoyo a dispositivos inalámbricos:** Hemos construido Kali Linux para que soporte tantos dispositivos inalámbricos como sea posible, permitiendo que funcione correctamente en una amplia variedad de hardware y hacerlo compatible con varios USB y otros dispositivos inalámbricos.

- **Kernel personalizado con parches de inyección:** Como probadores de penetración, el equipo de desarrollo a menudo tiene que hacer evaluaciones inalámbricas para que nuestro kernel tenga los últimos parches de inyección incluidos.

- **Entorno de desarrollo seguro:** El equipo de Kali Linux está compuesto por un pequeño grupo de personas de confianza que sólo puede comprometer e interactuar con los paquetes de los repositorios, haciendo uso de múltiples protocolos seguros.

- **Paquetes firmado con PGP y repos:** Todos los paquetes de Kali son firmados por cada desarrollador individualmente cuando se construyen y son comprometidos. Los repositorios posteriormente firman los paquetes también.

- **Multi-lenguaje:** Aunque las herramientas de penetración tienden a ser escritas en inglés, nos hemos asegurado de que Kali tenga soporte multilingüe, lo que permite a más usuarios poder operar en su idioma nativo y encontrar las herramientas necesarias para el trabajo.

- **Totalmente personalizable**: Estamos completamente consciente de que no todo el mundo estará de acuerdo con nuestras decisiones de diseño por lo que hemos hecho lo más fácil posible para nuestros usuarios más aventureros puedan personalizar Kali Linux a su gusto, todo el camino hasta el núcleo.

Link de VirtualBox

Download the latest version of VirtualBox from the official page
https://www.virtualbox.org/

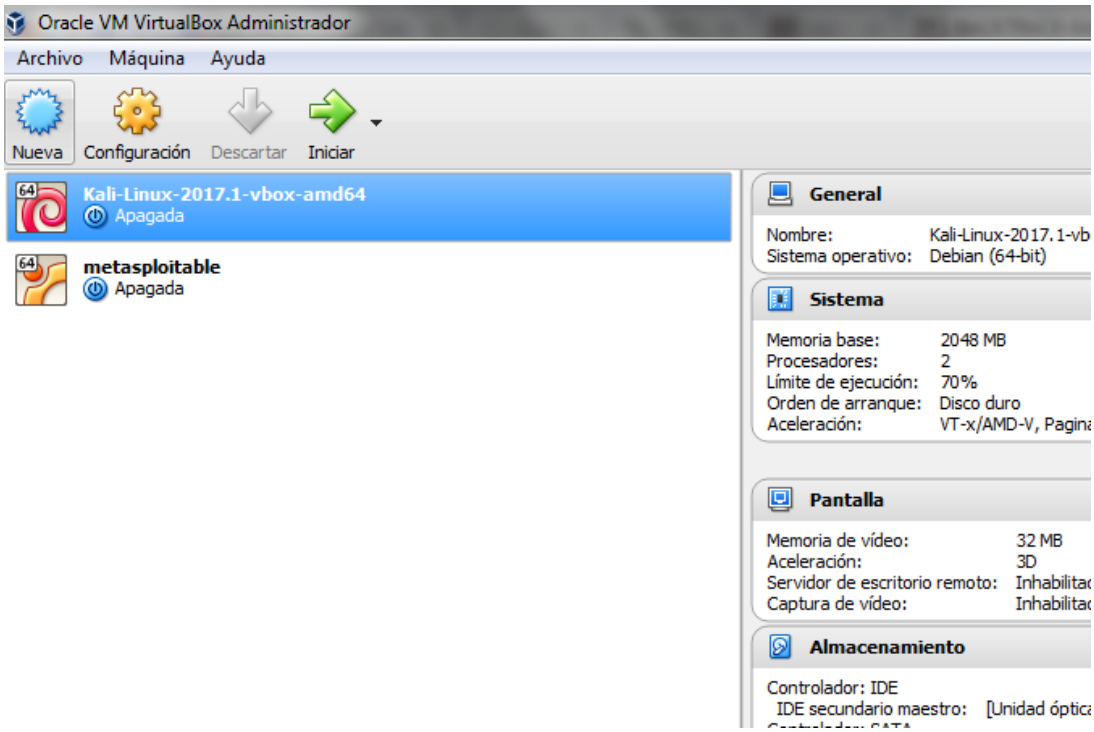
Link de Kali

- Bajar los ISO de Kali ISO desde el siguiente link.
- https://www.kali.org/downloads/

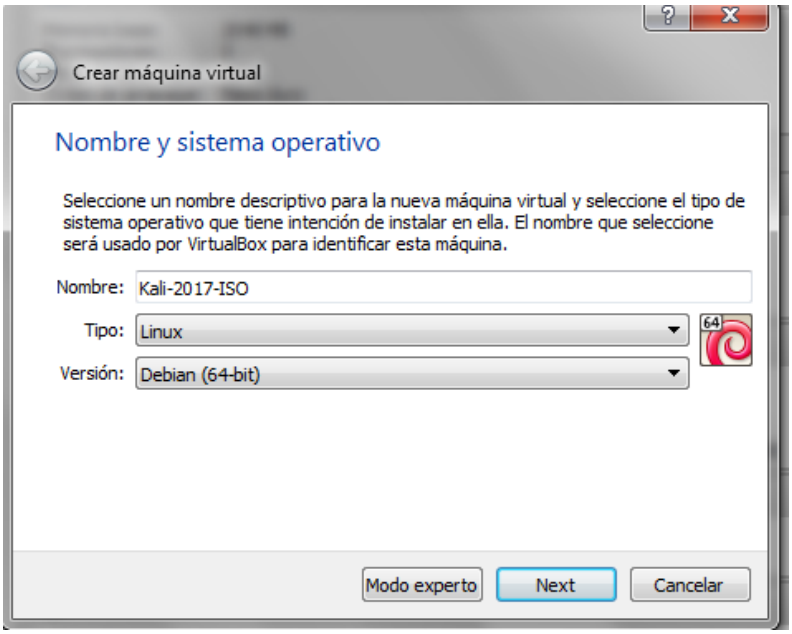
La versión a utilizar es la ISO “Kali 64 bit”

Configuración de VrtualBox

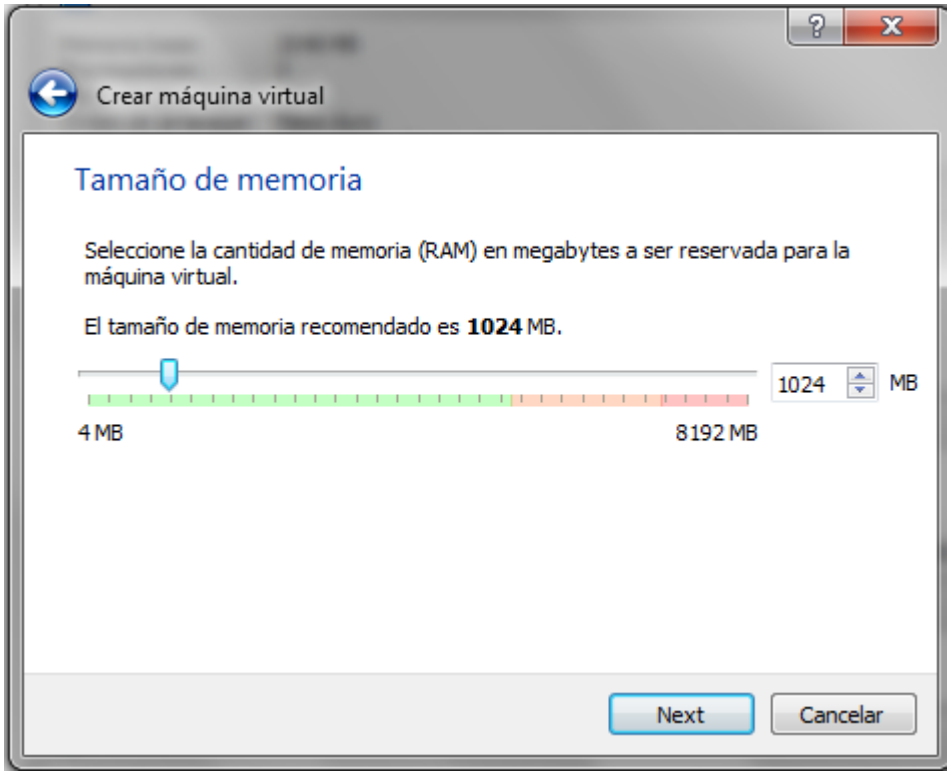
Desde la consola de VirtualBox vamos al icono de Nueva.



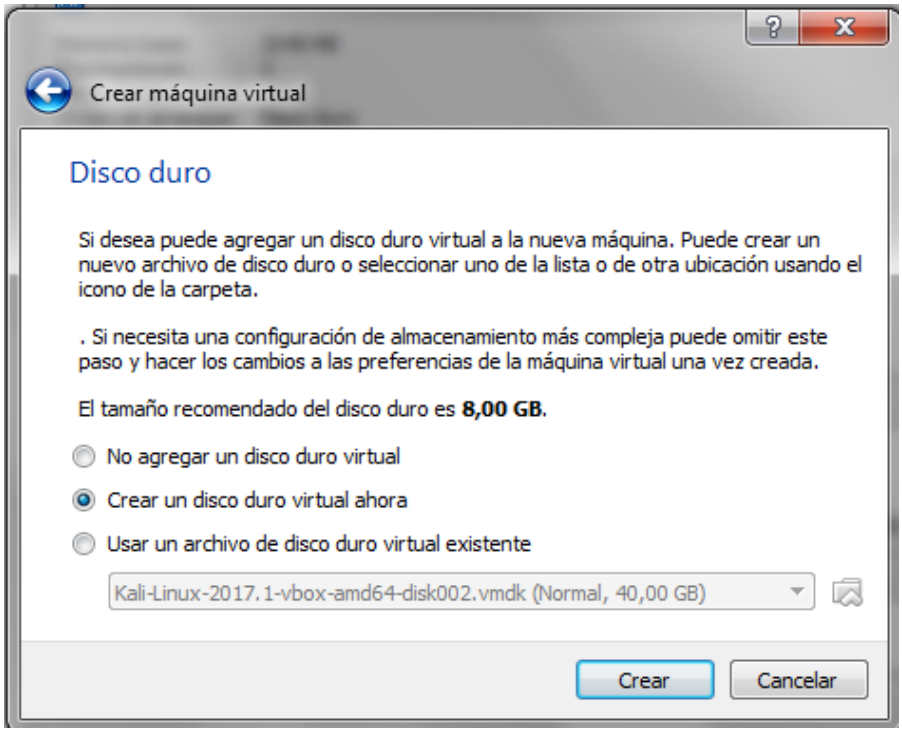
Se nos abrirá un manu donde debemos colocar el nombre de maquina virtual y el tipo de SO a instalar.



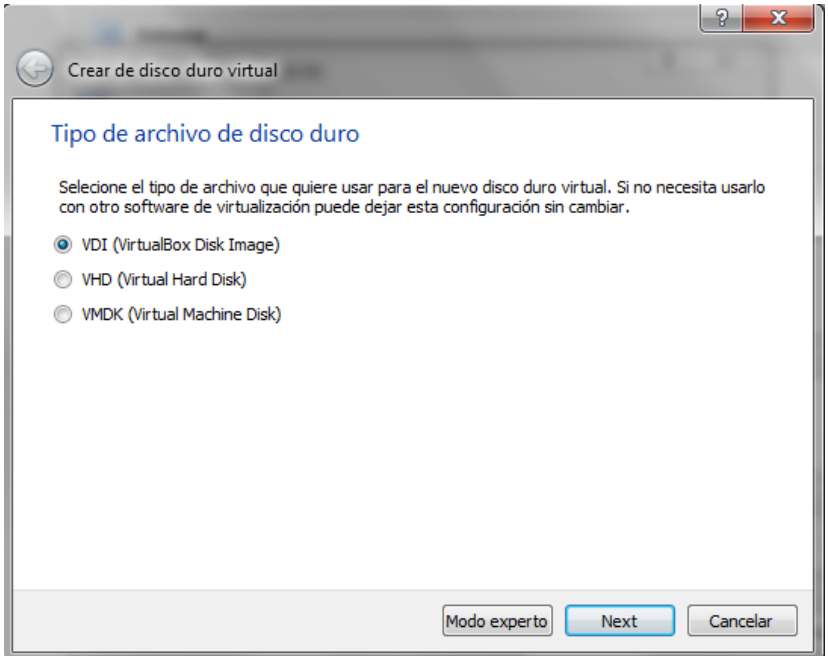
La memoria deben seleccionarla en función de su PC o Notebook, con 512MB de RAM es funcional para las practica.



Para la instalación desde una ISO es necesario crear un disco virtual donde se instalara localmente el SO.

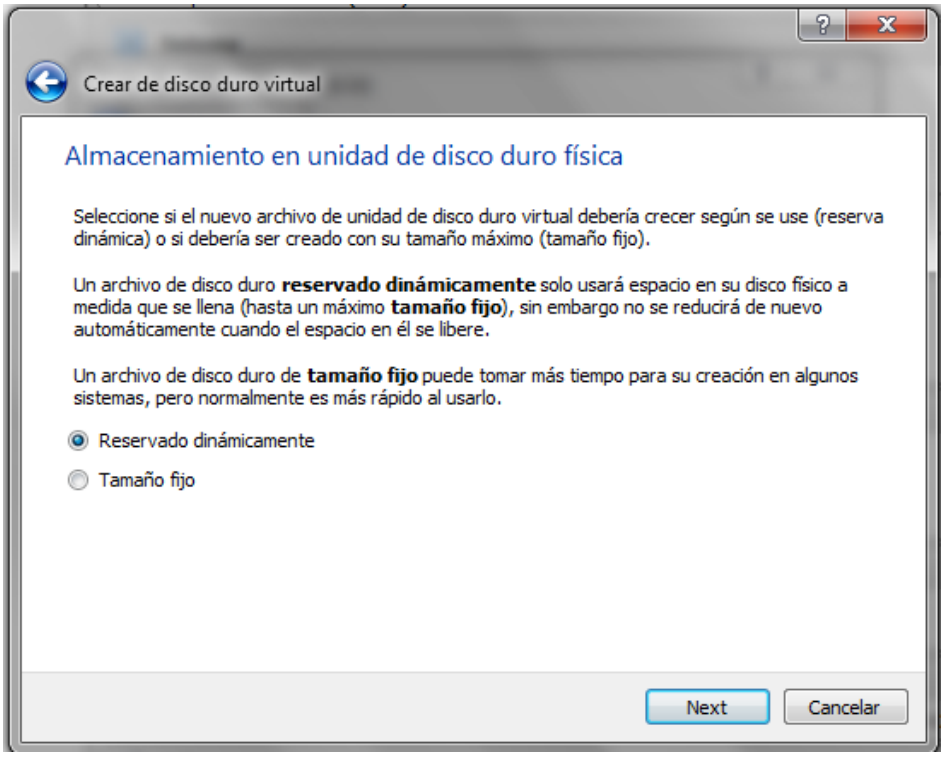


Si quieren copiar o llevar la maquina virtual a otra plataforma que no sea VirtualBox deben seleccionar la opción 2 para Hyper-V de Microsoft o la opción 3 VMDK para VMware.

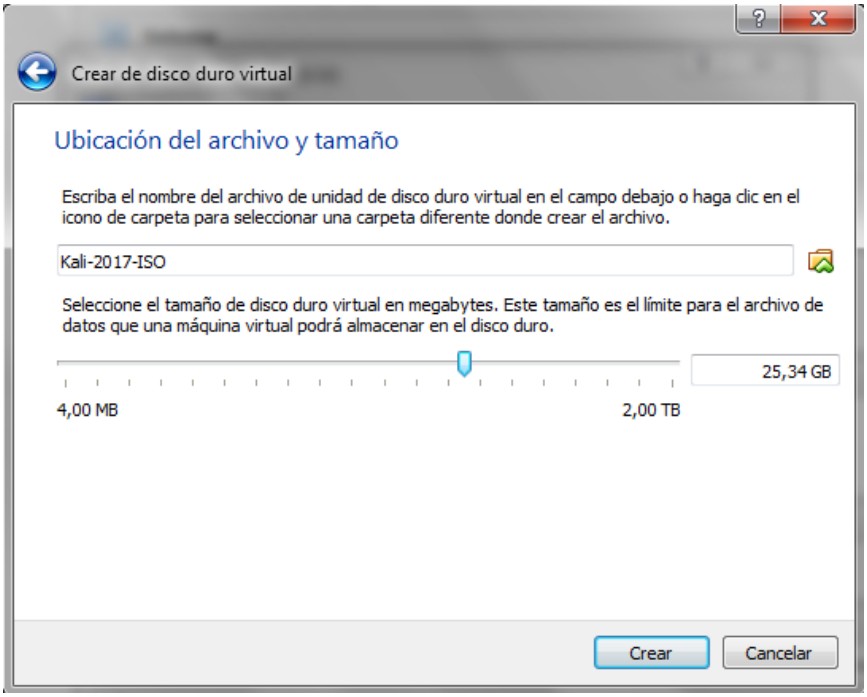


Este punto es muy importante ya que optimiza el espacio utilizado en disco.

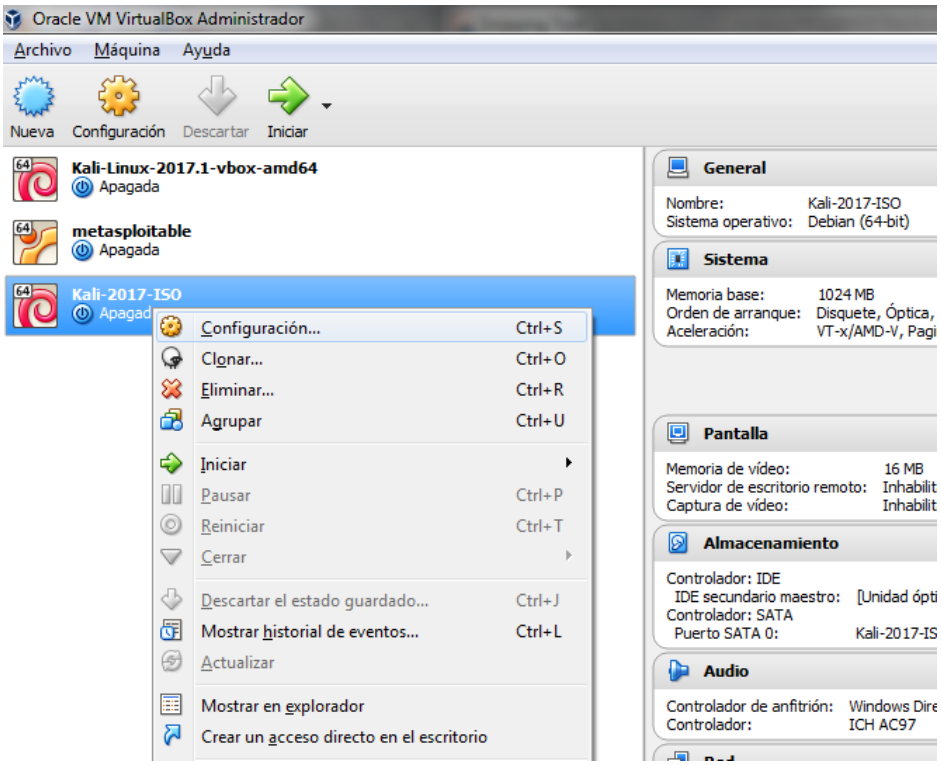
Utilizar “Reservado Dinámicamente”



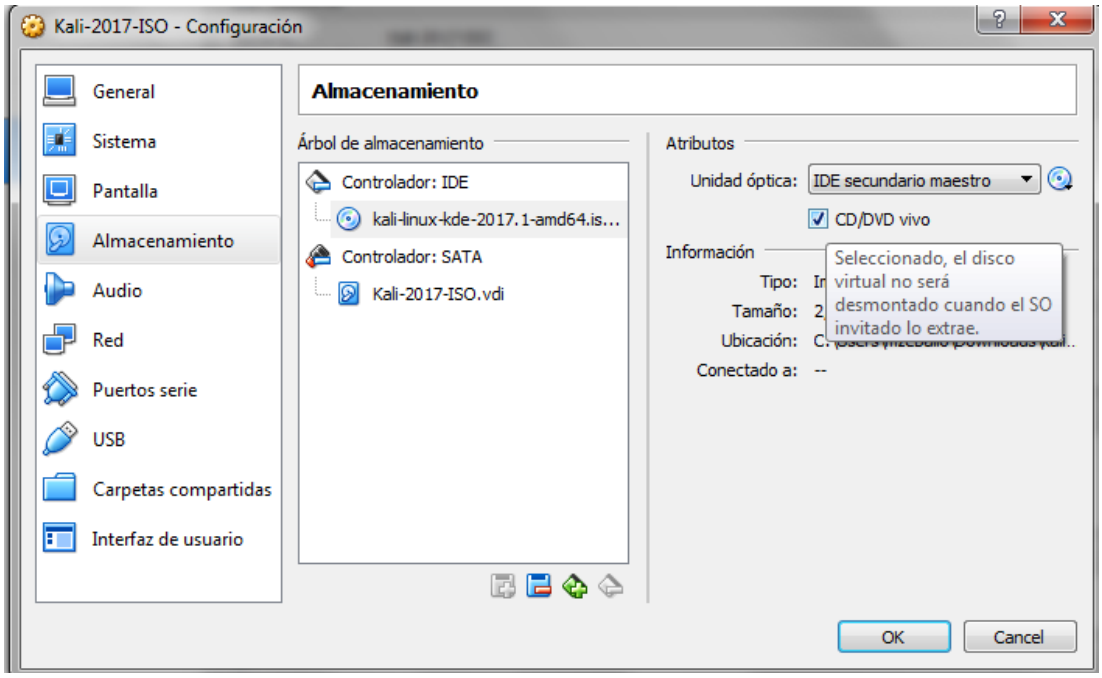
En este punto vamos a seleccionar el tamaño final del disco, digo final porque como elegimos la opción “Reservado Dinámicamente” el disco se va a ir llenando con la utilización del mismo.



Luego de crear la maquina virtual tenemos que configurarla para que en el inicio realice el boot desde la iso montada virtualmente como un DVD.

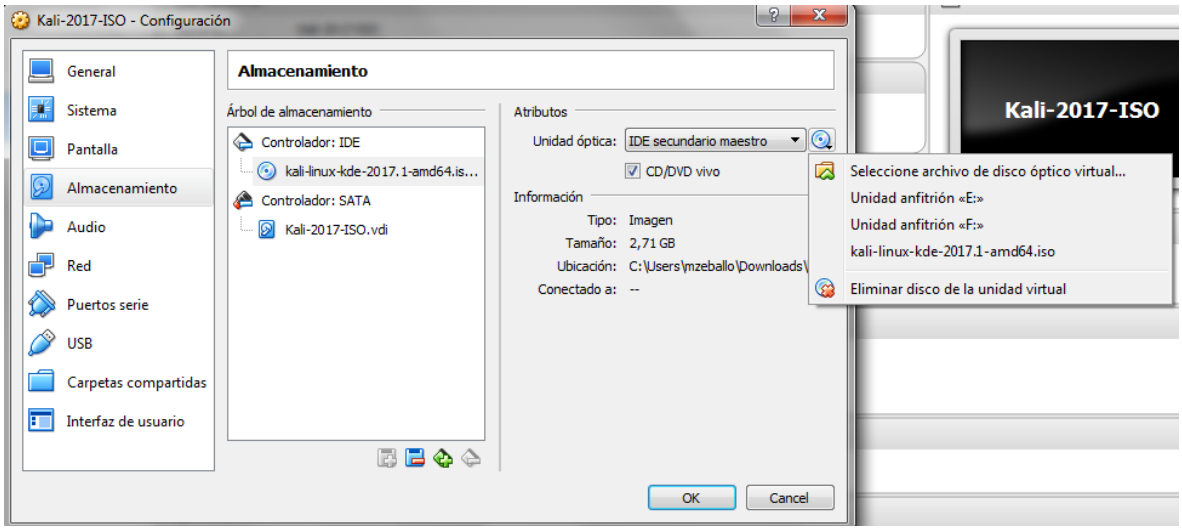


En la opción almacenamiento vamos a ir a cambiar los atributos de la unidad óptica.

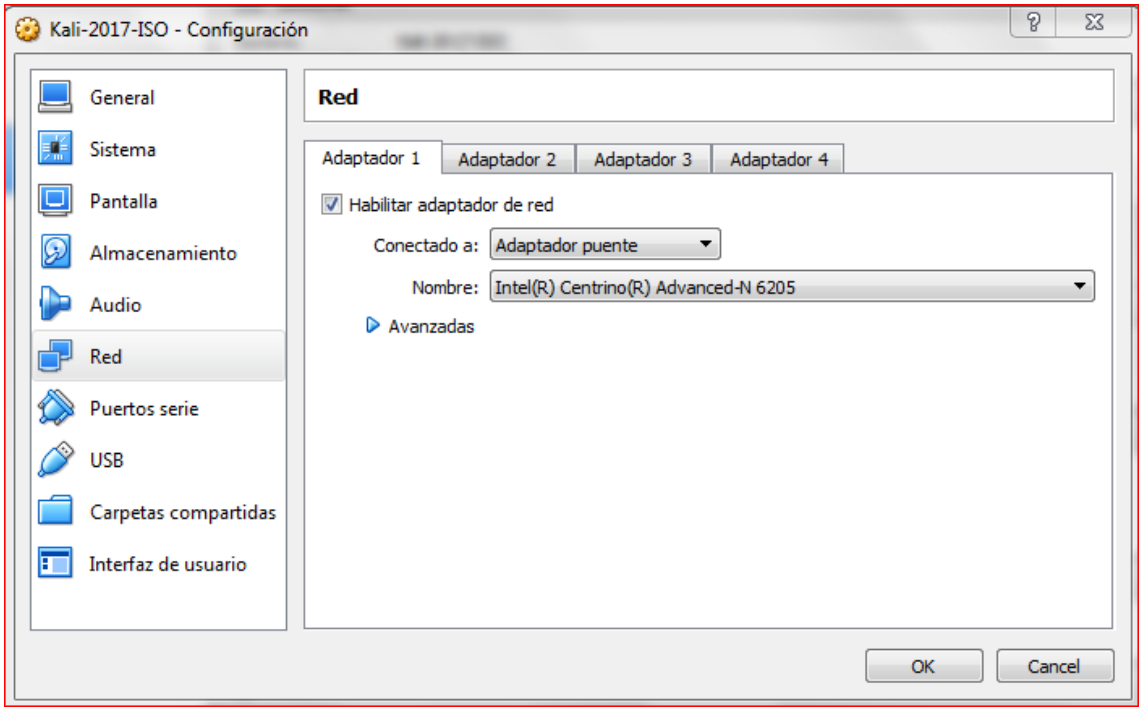


La opción de CD/DVD vivo debe estar tildada para que en el arranque lo haga desde el DVD/ISO

Haciendo click en el DVD nos va a dejar buscar la imagen ISO para montarla.



Las maquinas que usaremos en las practicas tienen que tener el adaptador Ethernet en modo puente (bridge).

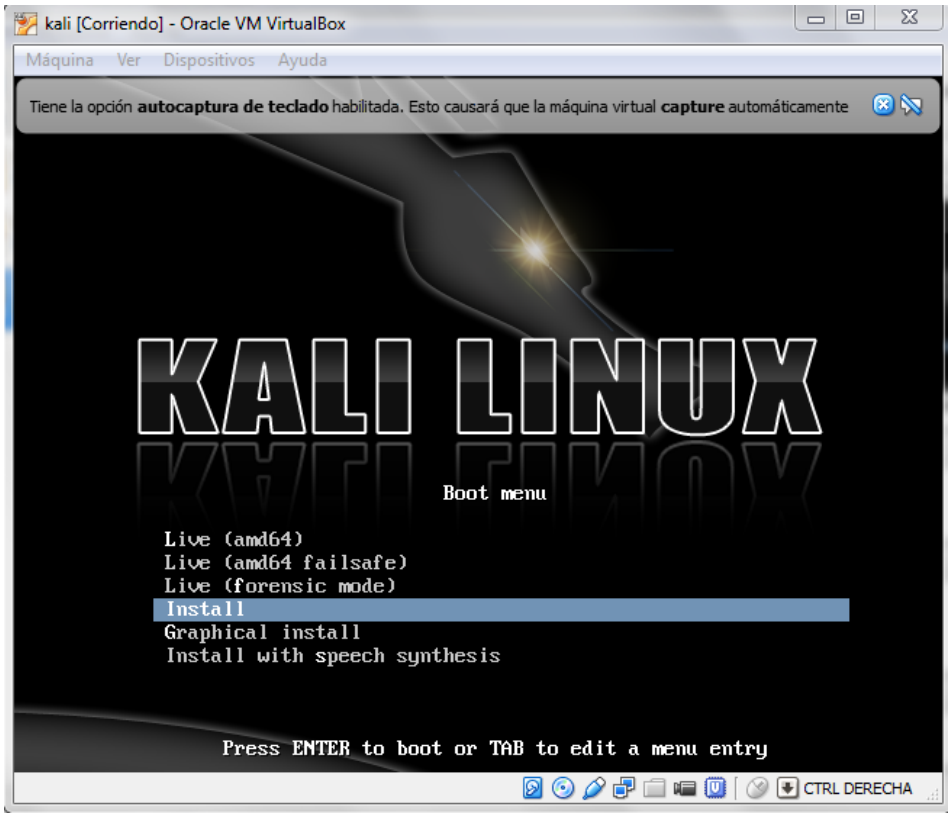


Luego de montar la imagen ISO, seleccionamos la maquina virtual creada y hacemos click en iniciar.

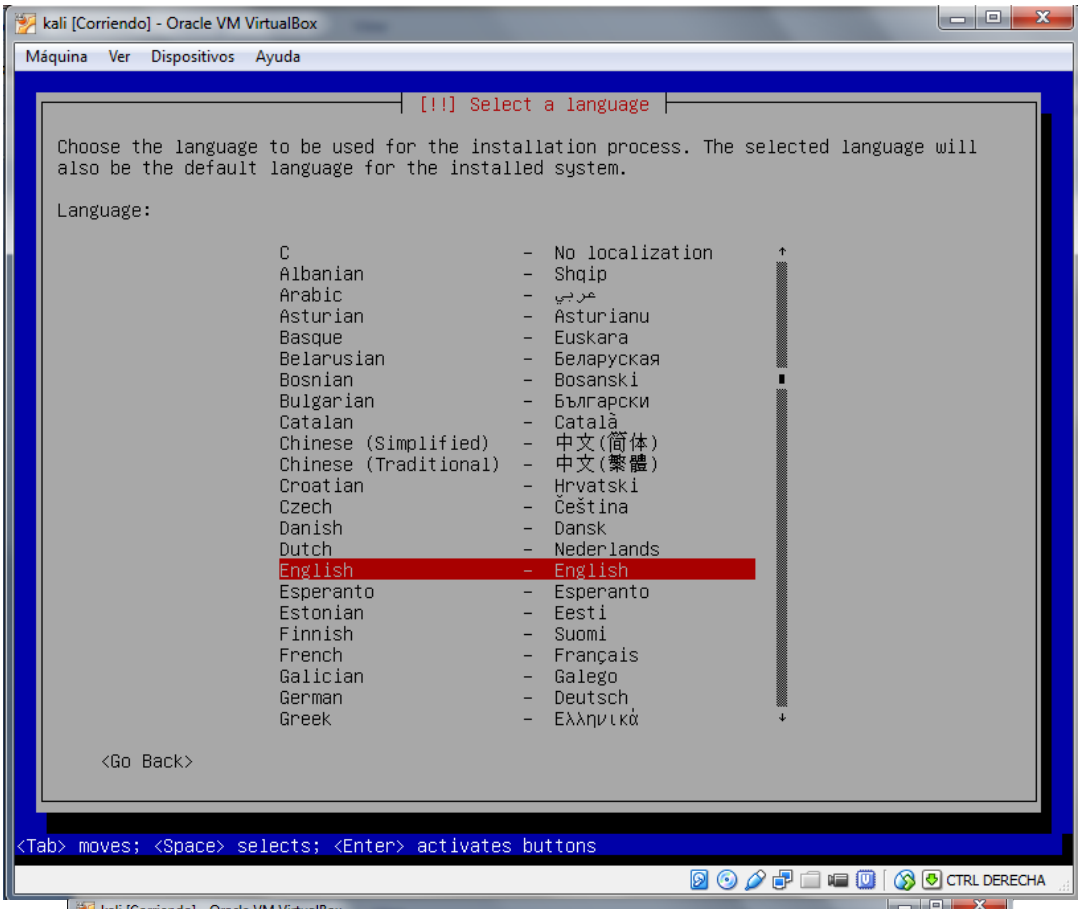
La velocidad de la instalación va a depender de los recursos de su PC.

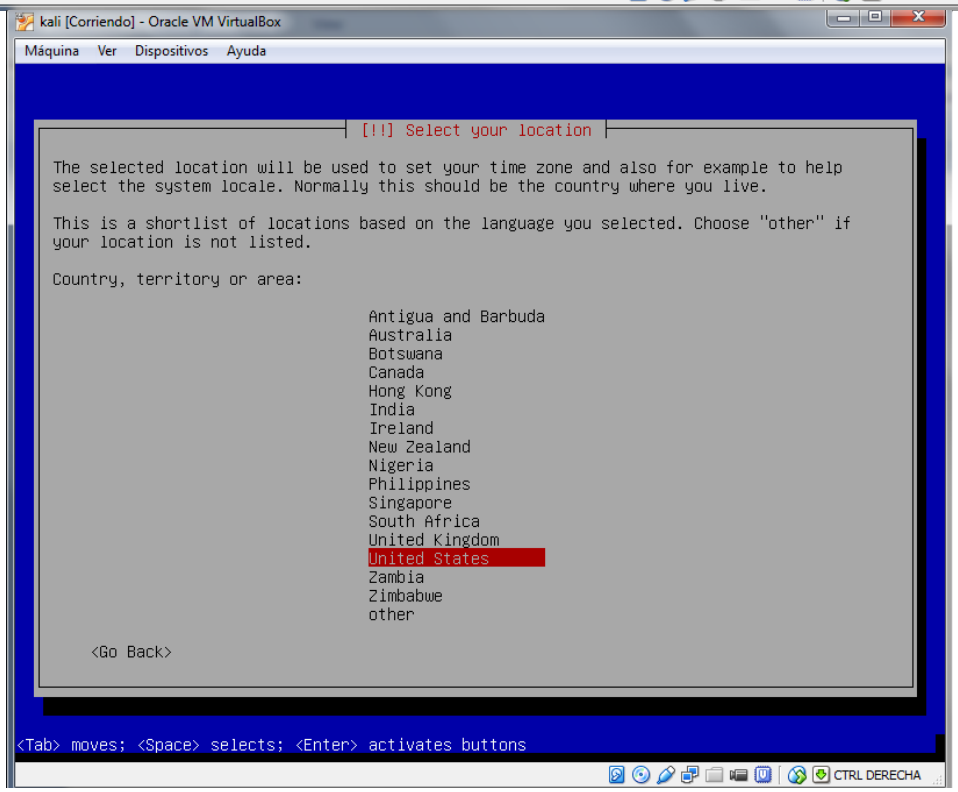
Comenzamos la instalación de Kali 2017.1

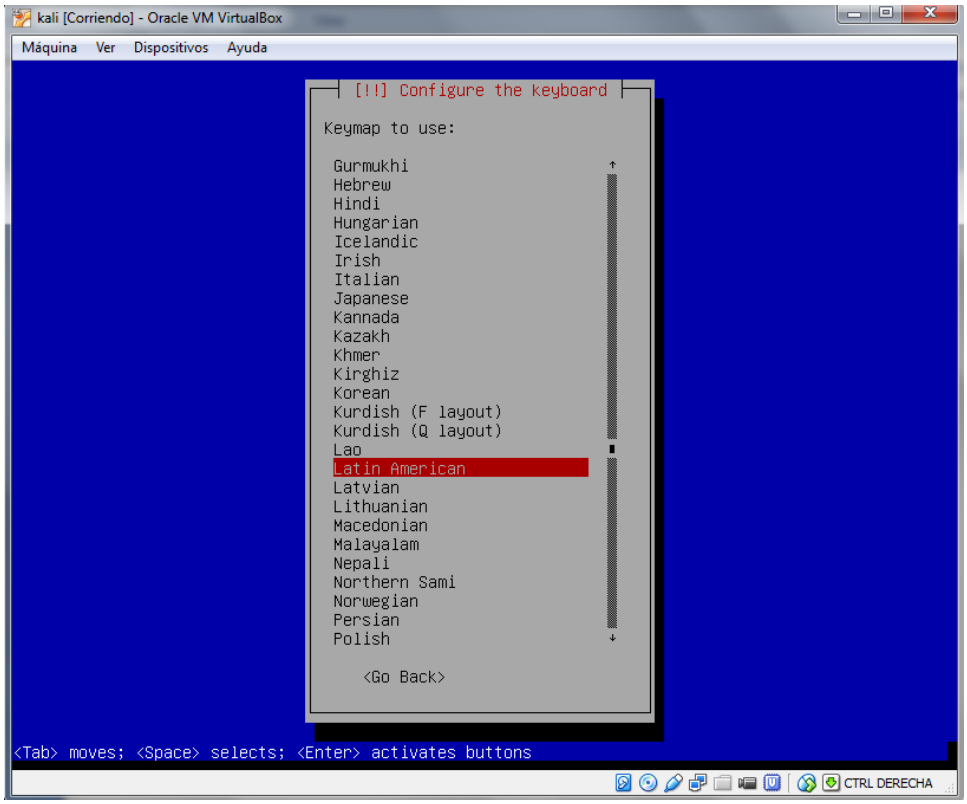
Pueden elegir la instalación Grafica o simple. En este ejemplo usaremos sin gráficos



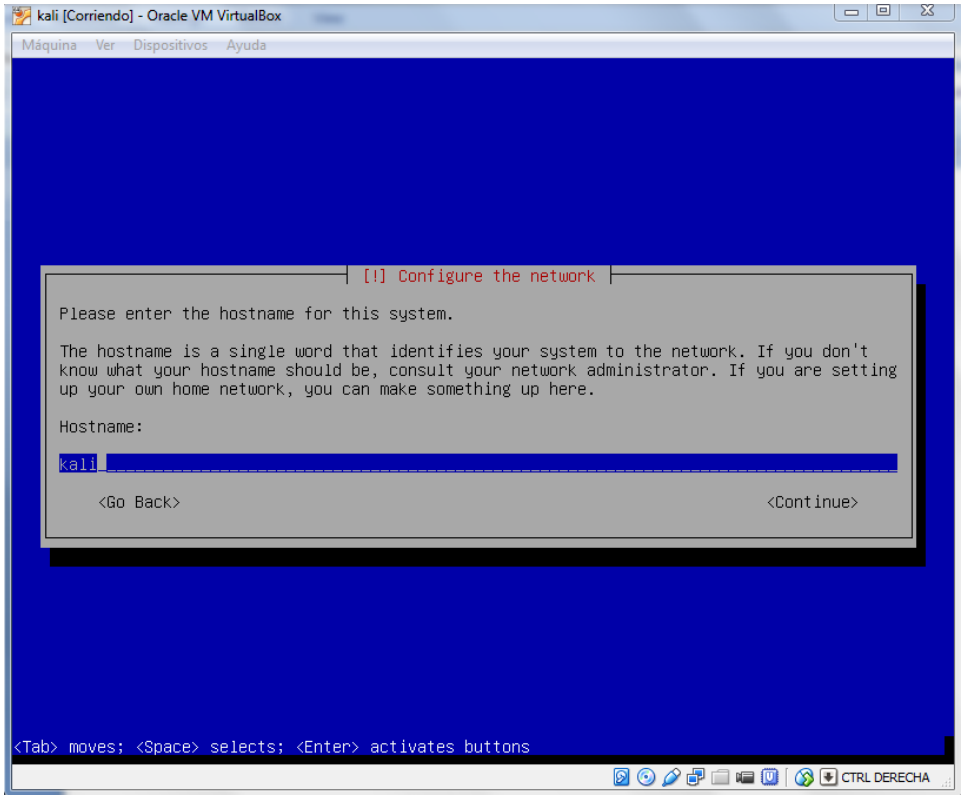
Seleccione el idioma que desee y luego su país de localización. También se le pedirá que configure su teclado con el mapa de teclado adecuado.


kali [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
[!!] Select a language
Choose the language to be used for the installation process. The selected language will also be the default language for the installed system.
Language:
C - No localization
Albanian - Shqip
Arabic - عربي
Asturian - Asturianu
Basque - Euskara
Belarusian - Беларуская
Bosnian - Bosanski
Bulgarian - Български
Catalan - Català
Chinese (Simplified) - 中文(简体)
Chinese (Traditional) - 中文(繁體)
Croatian - Hrvatski
Czech - Čeština
Danish - Dansk
Dutch - Nederlands
English - English
Esperanto - Esperanto
Estonian - Eesti
Finnish - Suomi
French - Français
Galician - Galego
German - Deutsch
Greek - Ελληνικά
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
CTRL DERECHA

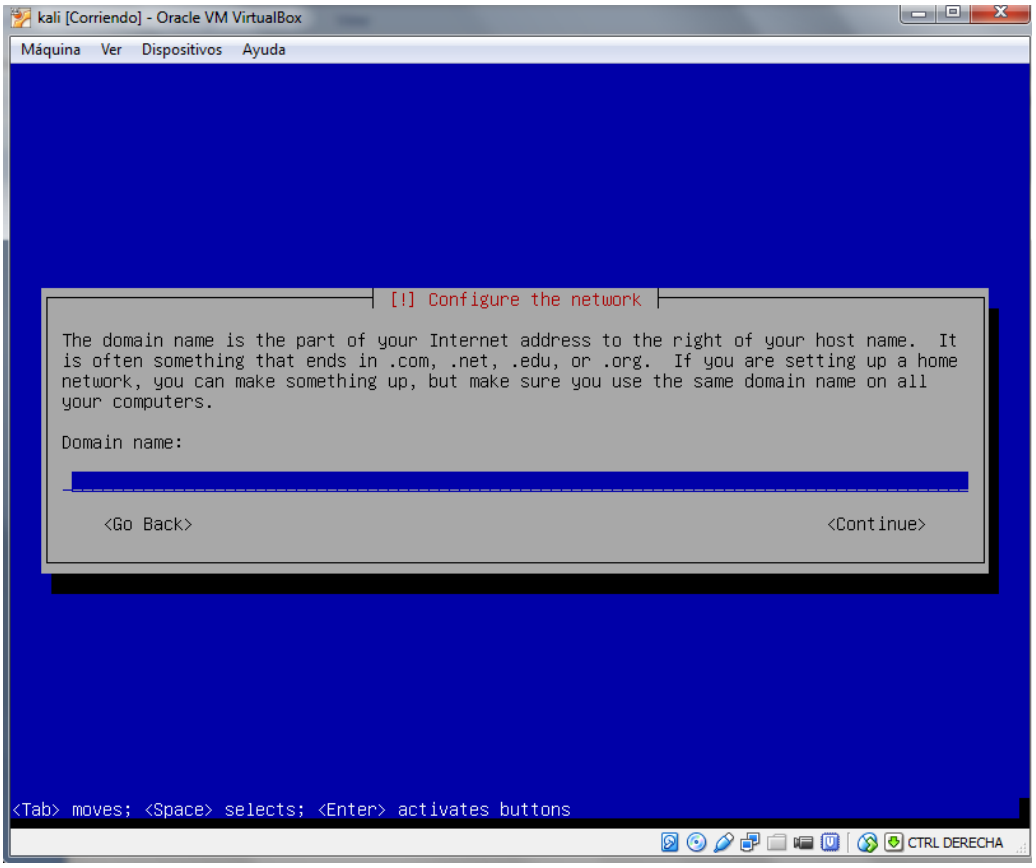

kali [Corriendo] - Oracle VM VirtualBox
Máquina Ver Dispositivos Ayuda
[!!] Select your location
The selected location will be used to set your time zone and also for example to help select the system locale. Normally this should be the country where you live.
This is a shortlist of locations based on the language you selected. Choose "other" if your location is not listed.
Country, territory or area:
Antigua and Barbuda
Australia
Botswana
Canada
Hong Kong
India
Ireland
New Zealand
Nigeria
Philippines
Singapore
South Africa
United Kingdom
United States
Zambia
Zimbabwe
other
<Go Back>
<Tab> moves; <Space> selects; <Enter> activates buttons
CTRL DERECHA



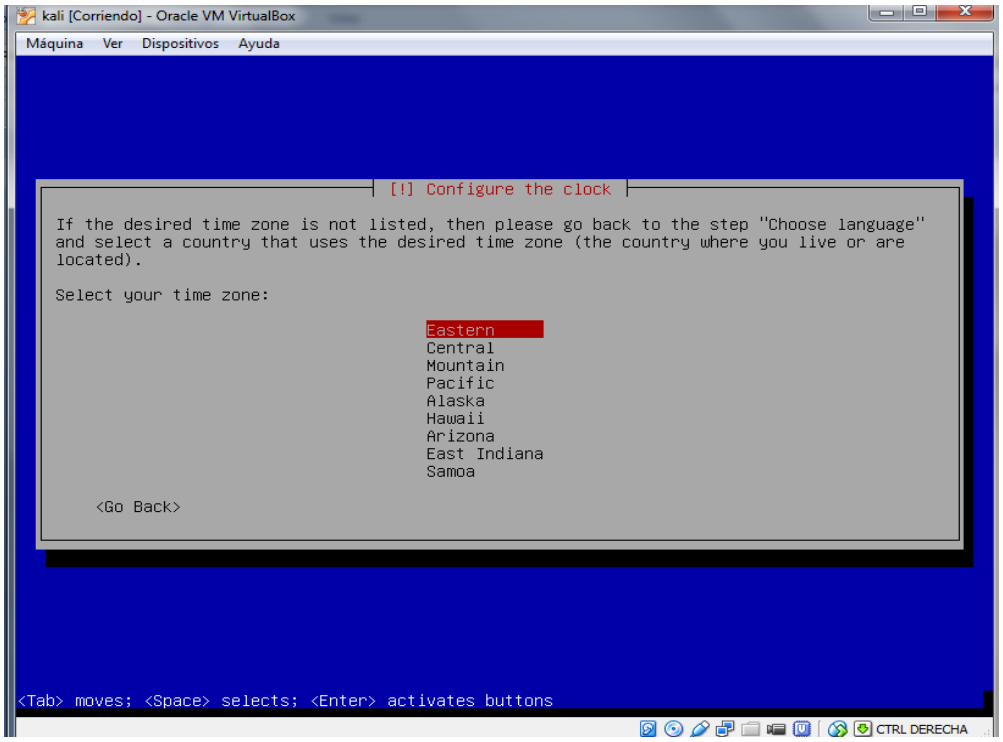
El programa de instalación copiará la imagen en su disco duro, probará las interfaces de red, y luego le pedirá que introduzca un nombre de host para el sistema. En el siguiente ejemplo, hemos escrito “Kali”, como el nombre de host.



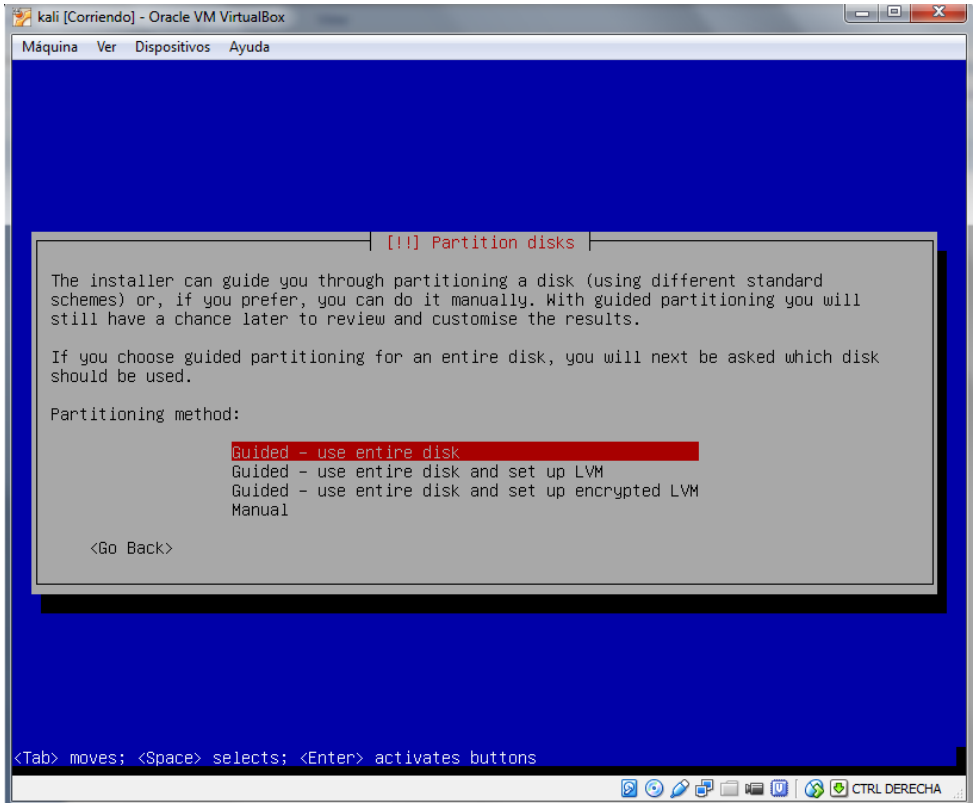
En domain name lo dejamos en blanco



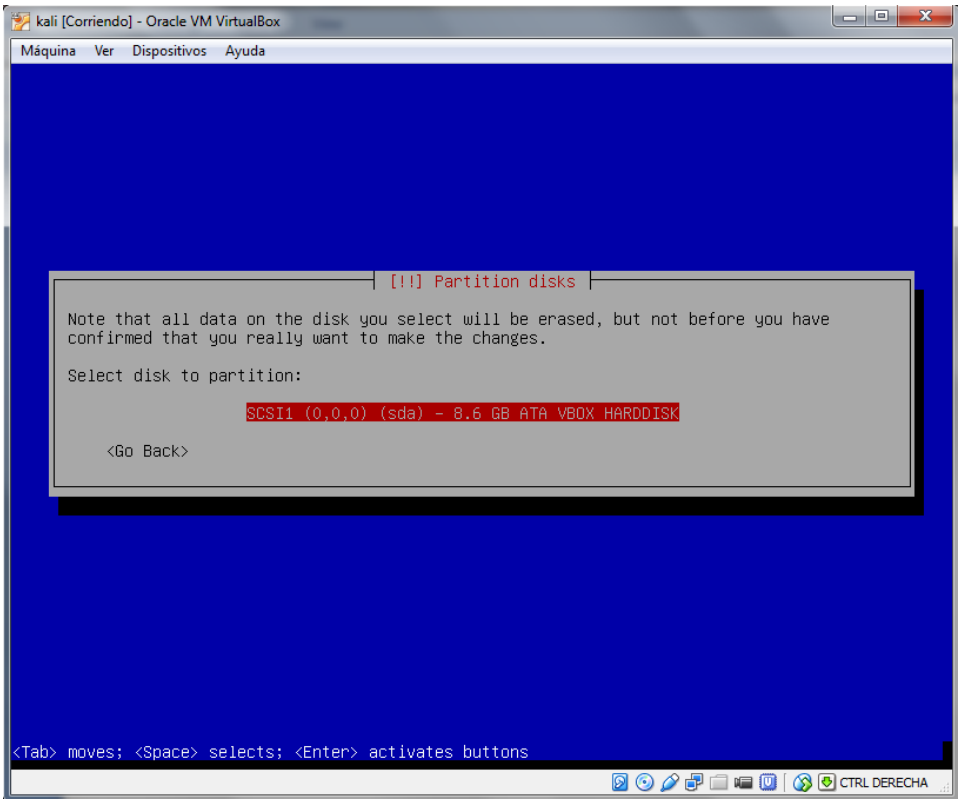
Configure su zona horaria.



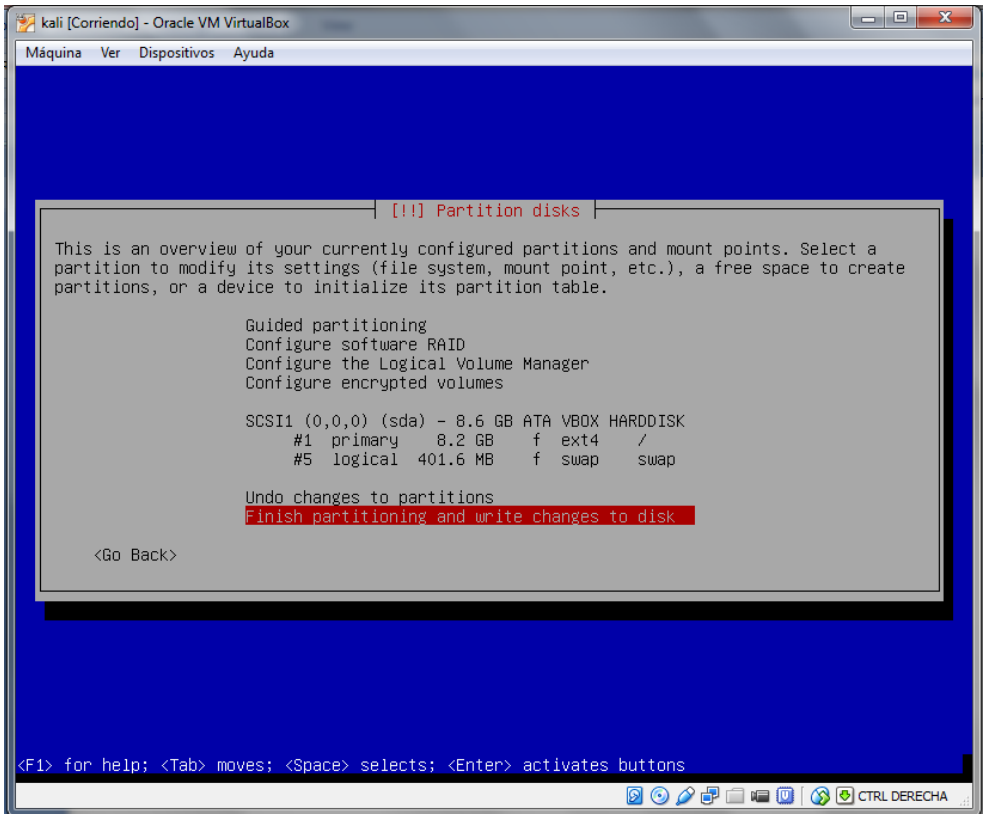
Para la configuración de las particiones de los discos vamos a optar por la opción guiada.



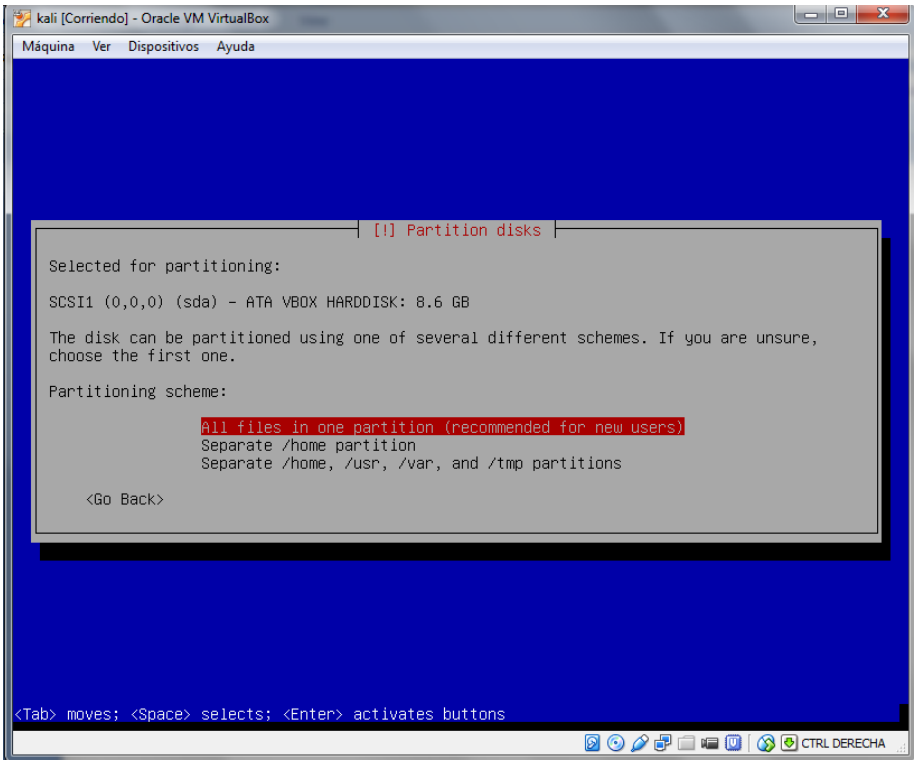
Nos va a informar que los datos serán borrados (el disco no tiene datos)



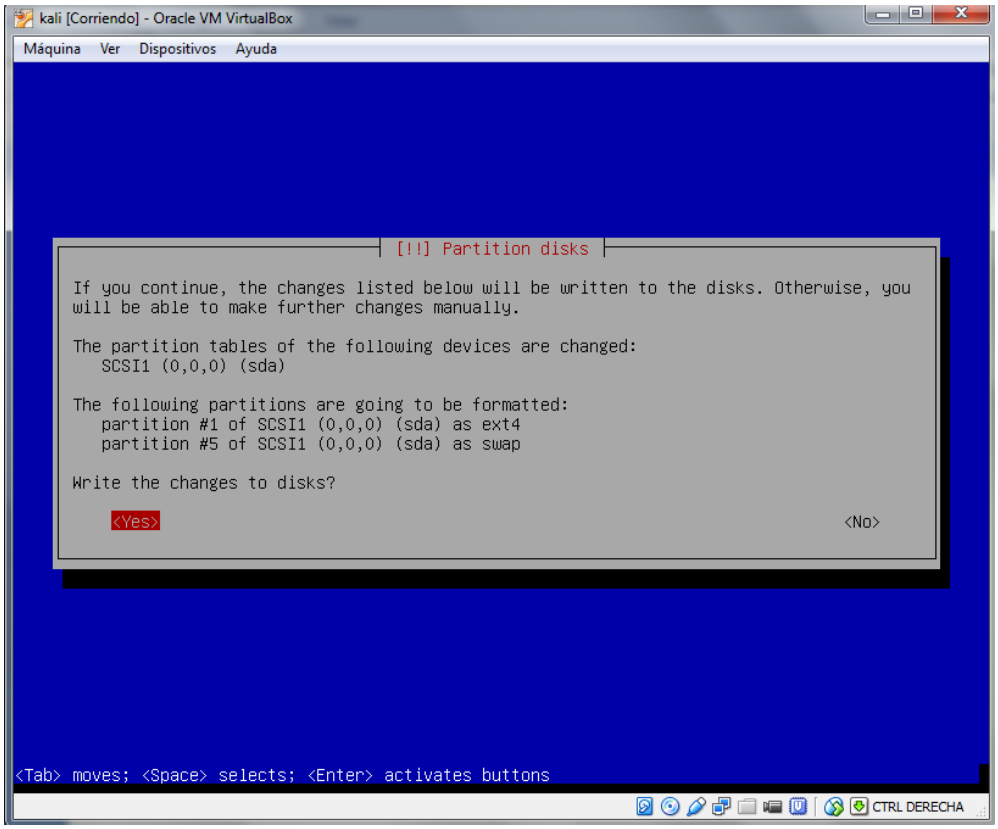
Dejamos todo por default y finalizamos el particionamiento de los discos.



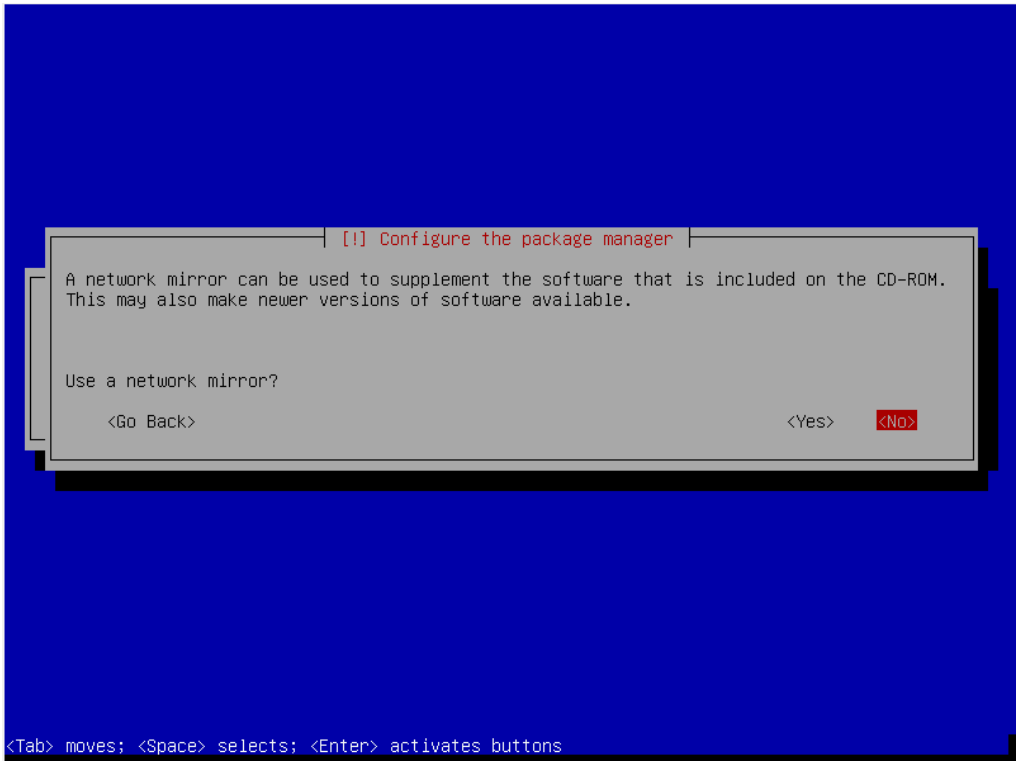
Usaremos la opción de tener todos los archivos en una partición.



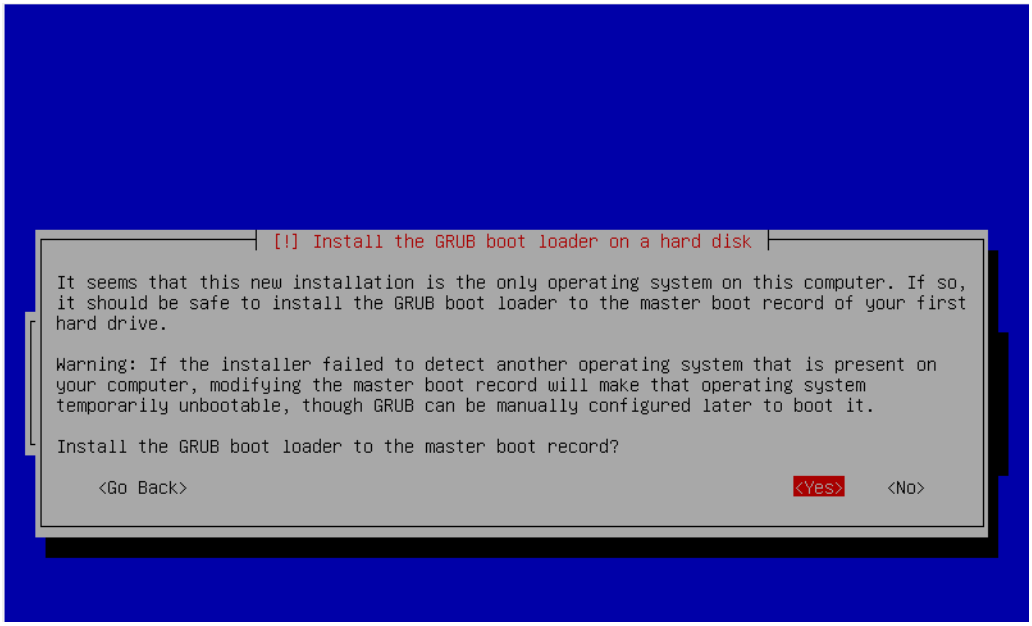
<Yes> para guardar los cambios



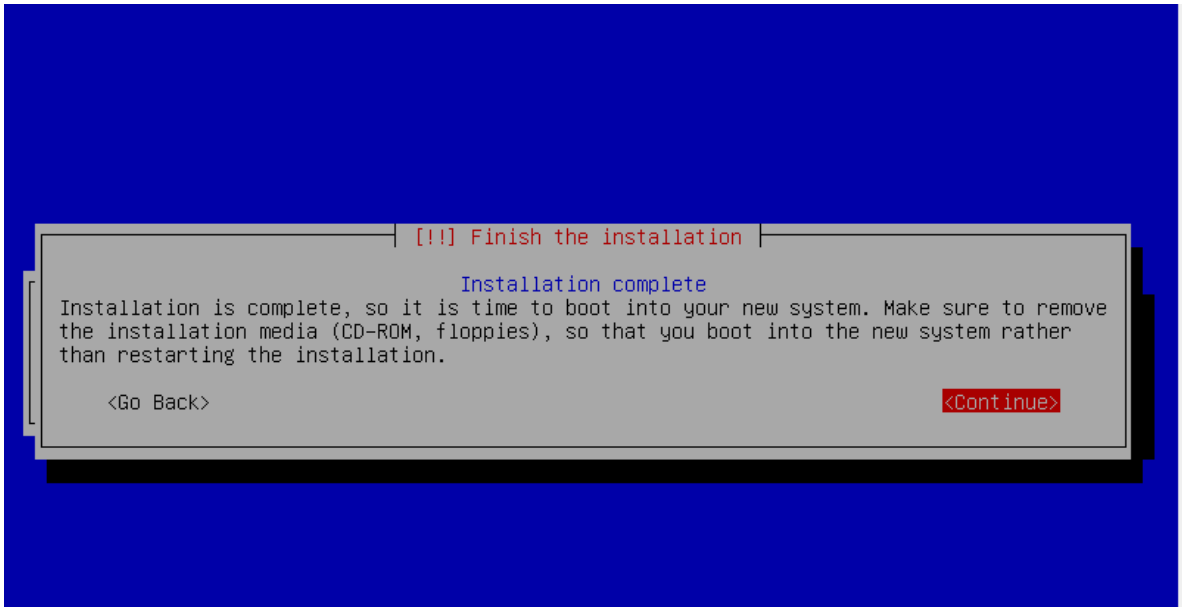
No usaremos mirror del SO, esta opción te permite bajar e instalar paquetes online



Daremos ok a instalar GRUB



Fin de la instalación!!!



Importante!!!

Luego de finalizar la instalación hay que sacar el tilde del DVD vivo. De lo contrario va a iniciar desde al DVD virtual.

Recordar que para ingresar a Kali luego de bootear el user es **Root** y la password **toor** o la que decidieron ustedes en la instalación.

Desde la consola de Linux probar los siguientes comandos básicos:

Para der por finalizada la primer practica ejecutar los comandos desde la consola de Kali y enviarme las salidas en un documento para formalizar y dar por aprobada la práctica.

ls

list: listar. Nos muestra el contenido de la carpeta que le indiquemos después. Por ejemplo. Si queremos que nos muestre lo que contiene /etc:

ls /etc

Si no ponemos nada interpretará que lo que queremos ver es el contenido de la carpeta donde estamos actualmente:

ls

Para mostrar todos los archivos y carpetas, incluyendo los ocultos:

ls -a

Para mostrar los archivos y carpetas junto con los derechos que tiene, lo que ocupa, etc:

ls -l

Si quisiéramos mostrar los archivos de la misma forma que antes, pero que muestre también los ocultos:

ls -la

---

cd

change directory: cambiar directorio. Podemos usarlo con rutas absolutas o relativas. En las absolutas le indicamos toda la ruta desde la raíz (/). Por ejemplo, estemos donde estemos, si escribimos en consola…

cd /etc/apt …nos llevará a esa carpeta directamente.
cd / …nos mandará a la raíz del sistema de ficheros.

Las rutas relativas son relativas a algo, y ese algo es la carpeta donde estemos actualmente. Por ejemplo si estamos en /home y queremos ir a una carpeta que se llama temporal dentro de nuestra carpeta personal.

cd tu_carpeta/temporal

Hemos obviado el /home inicial ya que si no lo introducimos toma como referencia el directorio donde estamos.

cd

Esto lo que hace es que te lleva a tu carpeta personal directamente y estemos donde estemos, es algo realmente muy práctico, muy simple y que no todos conocen.

---

mkdir

make directory: hacer directorio. Crea una carpeta con el nombre que le indiquemos. Podemos usar rutas absolutas y relativas. Podemos indicarle toda la ruta que le precede al directorio que queremos crear, o si estamos ya en la carpeta que lo va a contener basta con poner tan sólo el nombre:

mkdir /home/tu_cuenta/pepino

Si ya estamos en /home/tu_cuenta…

mkdir pepino

---

rm

remove: borrar. Borra el archivo o la carpeta que le indiquemos. Como antes se puede indicar la ruta completa o el nombre del archivo. Esto a partir de ahora lo vamos a obviar, creo que ya ha quedado claro con los dos comandos anteriores.

Para borrar un archivo: #rm nombre_archivo

Para borrar una carpeta vacía: #rm nombre_carpeta

Para borrar una carpeta que contiene archivos y/o otras carpetas:

#rm -r nombre_carpeta

Otras opciones: “-f” no pide una confirmación para eliminar o “-v” muestra lo que borra.

---

cp

copy: copiar. Copia el archivo indicado donde le digamos. Aquí podemos también jugar con las rutas, tanto para el fichero origen, como en el del destino. También se puede poner el nombre que se le quiere dar a la copia. Por ejemplo, si estuviéramos en /etc/X11 y quisiéramos hacer una copia de seguridad de xorg.conf en nuestra carpeta personal:

cp xorg.conf /home/tu_carpeta/xorg.conf.backup

---

mv

move: mover. Es igual que el anterior, sólo que en lugar de hacer una copia, mueve directamente el archivo con el nombre que le indiquemos, puede ser otro distinto al original:

mv /etc/pepino.html /home/tu_carpeta/ese_pepino.html

Otro uso muy práctico que se le puede dar es para renombrar un archivo. Basta con indicar el nuevo nombre en el segundo argumento con la misma ruta del primero. En este ejemplo suponemos que ya estamos en la carpeta que lo contiene:

mv pepino.html ese_pepino.html

---

find

find: encontrar. Busca el archivo o carpeta que le indiques:

find / -name pepino

El comando anterior buscaría en todos los sitios las carpetas y archivos que se llamen pepino. Si tuviéramos la seguridad de que se encuentra en /var por ejemplo, se lo indicaríamos:

find /var -name pepino

Si no estamos muy seguros del nombre podemos indicárselo con comodines. Supongamos que el nombre de lo que buscamos contiene “pepi”, en la misma carpeta de antes:

find /var -name *pepi*

Tiene otras opciones. Por ejemplo podemos decirle que encuentre los archivos/carpetas de más de 1500 KB:

find / -size +1500

O los archivos/carpetas contienen el nombre “pepi” y tienen menos de 1000 KB:

find / -name *pepi* -size -1000

---

clear

clear: despejar. Limpia la pantalla/consola.

clear

---

ps

process status: estado de los procesos. Nos muestra lo que queramos saber de los procesos que están corriendo en nuestro sistema. Cada proceso está identificado con un número llamado PID. Si colocamos…

ps -A

…nos mostrará un listado de todos los procesos, su PID a la izquierda y su nombre a la derecha. Si queremos más información:

ps aux

---

kill

kill: matar. Elimina el proceso que le indiquemos con su PID:
kill

En ocasiones el proceso no “muere” del todo, pero se le puede forzar al sistema para que lo mate con seguridad del siguiente modo:

kill -9

---

sudo

super-user do: hacer como superusuario. La cuenta de usuario en Ubuntu es relativamente normal. Tiene derechos de administrador a medias. Me explico, los tiene, pero cada vez que se haga algo importante y de riesgo para el sistema, hay que hacerlo mediante el prefijo “sudo” y escribiendo después la contraseña.

Por ejemplo, algo que hemos hecho muchas veces en los tutoriales es hacer una copia de seguridad del fichero xorg.conf. Éste está localizado en la carpeta /etc/X11 y ahí ningún usuario puede hacer modificaciones o borrar nada si no es el administrador o tiene derechos como tal, gracias a sudo. Por eso hacíamos siempre:

sudo cp /etc/X11/xorg.conf /etc/X11/xorg.conf

Siempre que necesitemos hacer un apt-get/aptitude update o install y acciones de este tipo, tendremos que poner antes el “sudo”.

---

passwd

password: contraseña. Con este comando podremos cambiar la contraseña de nuestra cuenta. Primero nos pedirá la contraseña actual como medida de seguridad. Después nos pedirá que introduzcamos dos veces seguidas la nueva contraseña.

passwd

---

su

super-user: superusuario. Mediante ‘su’ podremos loguearnos como superusuario. Tras escribirlo nos pedirá la contraseña de root y estaremos como administrador.

su

Este comando también nos permite hacer login con otra cuenta distinta. Por ejemplo, imaginemos que tenemos otra cuenta, además de root y la nuestra, llamada “invitado”. Para hacer login como tal bastaría con poner:

su invitado

y después escribir la contraseña de esa cuenta.

sudo passwd

Gracias a la unión de estos dos comandos se puede cambiar la contraseña de root (la del super-usuario).

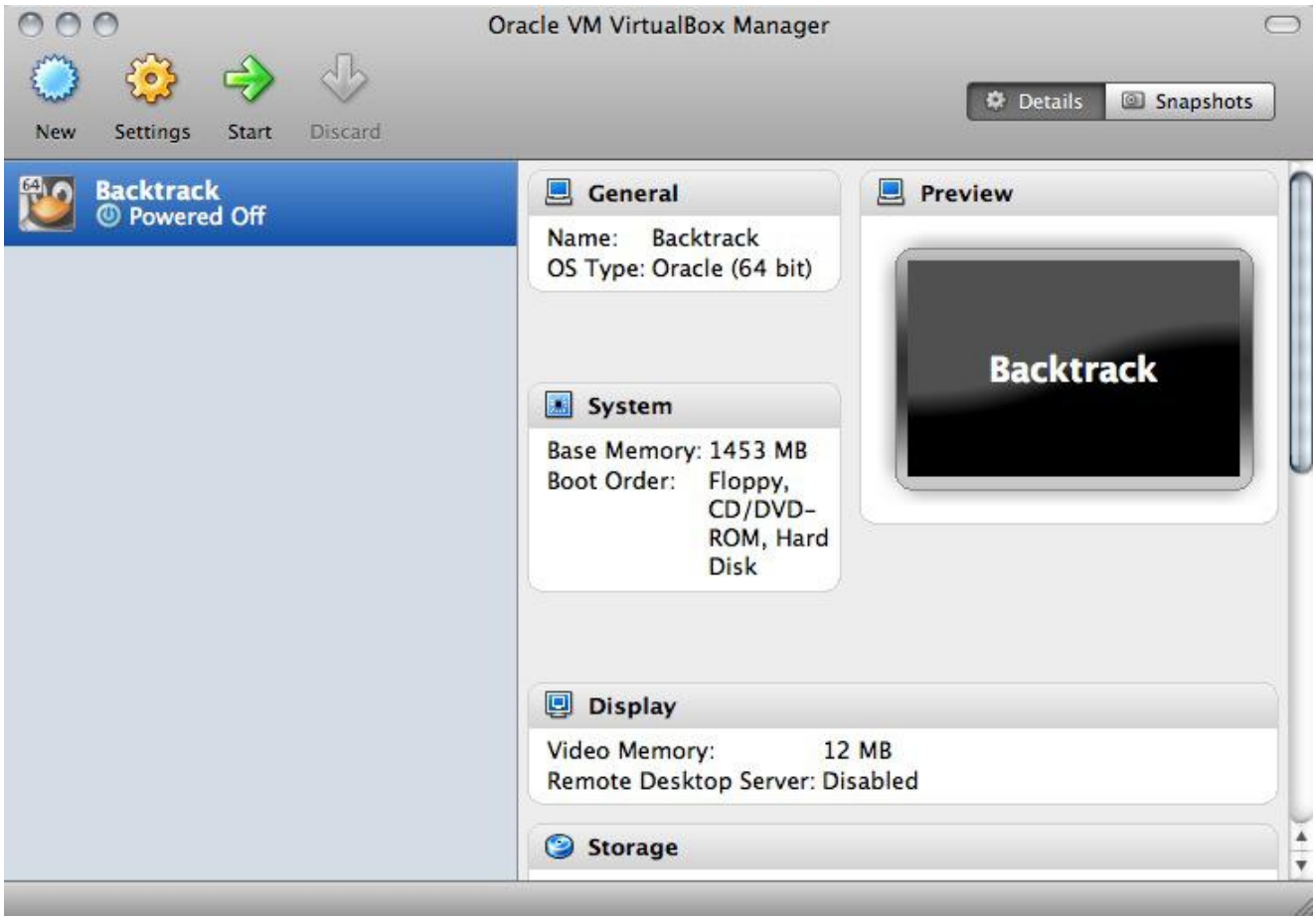
sudo passwd

Dejo esta implementación de backtrack el predecesor de Kali solo como muestra, no hay que instalarlo.

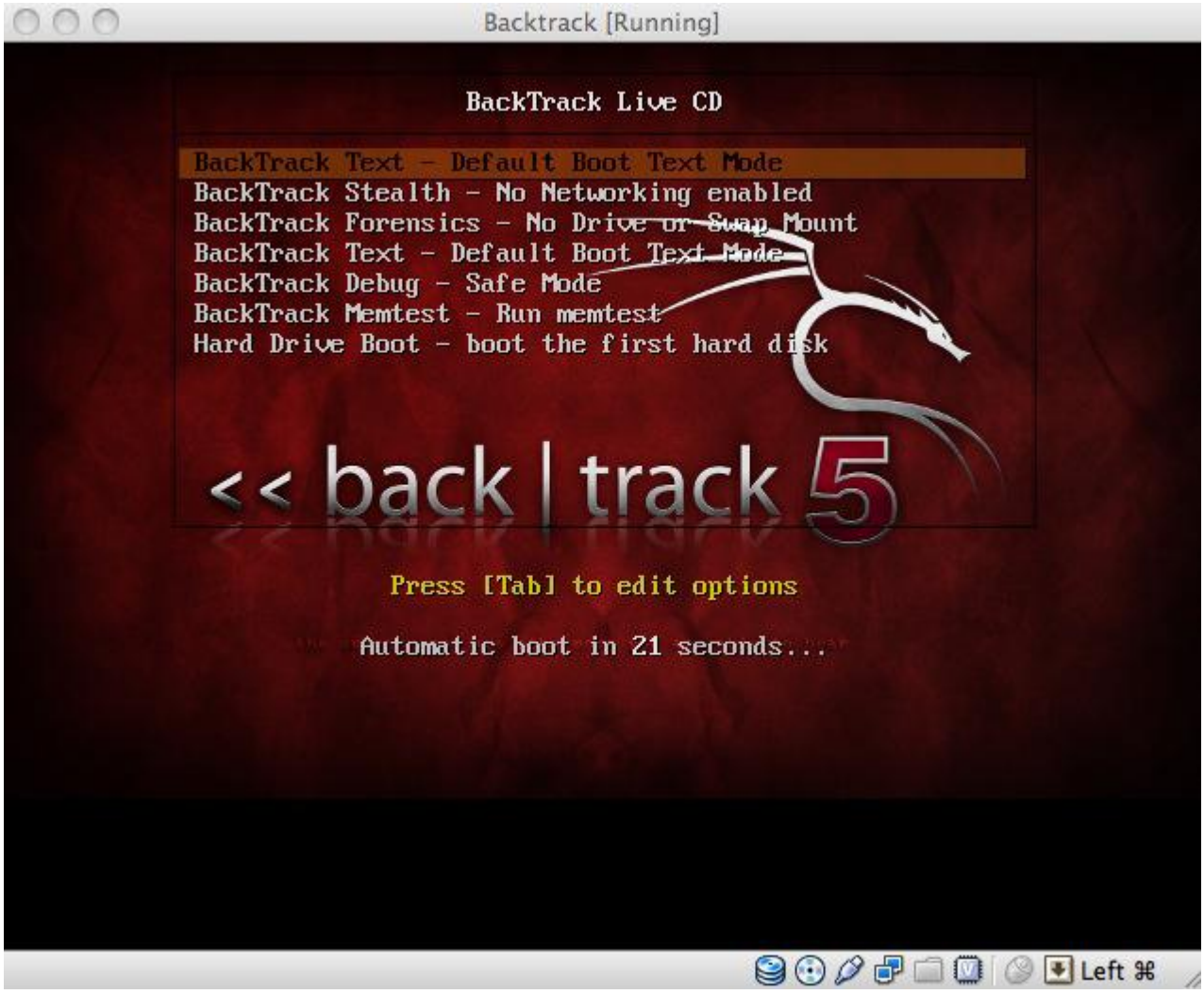

```
Click New ->Continue -> Next
Name (Select Ubuntu 64Bit) -> Next
Select Ram (Assign at least 30%)  -> Next
Check "Boot Disk" à Create New Hard Disk
Continue -> "Dynamically Expanding Storage" -> Choose Location -> Size
(Minimum of
Continue -> Done
```

- Your Disk Configuration should look similar to this:

Click Settings (We are going to leave mosts defaults on for everything for this How-To)
Click Storage à With "IDE Storage" Selected click the Drive Icon with the plus sign on it à
Choose Add CD/DVD à Choose Disk à Navigate to the BT5 ISO you had downloaded
Click Display and assign at least 64MB
Click Ok
Open Terminal and enter the Following
VboxManage setextradata "Backtrack" "CustomVideoMode1" "1100x740x16"



Click Start
Click inside the window -> Tab -> Choose "Backtrack Text"



- Once the boot sequence completes you will already be in a root shell.

'*NOTE**: If you have chosen the KDE Environment do not forget to issue the following command before* **startx**:

```
root@bt:~# rm /root/.kde/cache-*
```

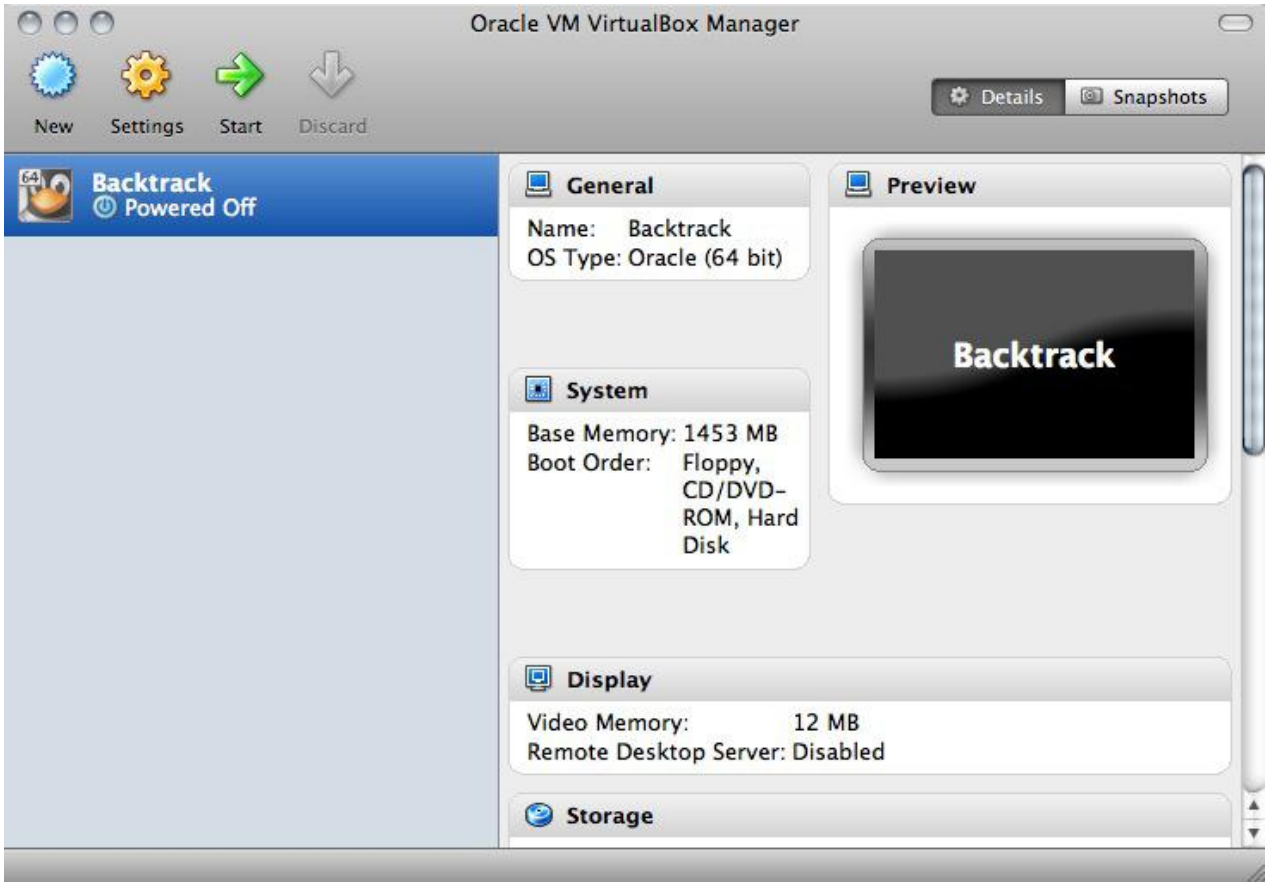
- Once Backtrack Launches Double Click the "Install Backtrack Icon" and follow the steps from here.
- After the setups is finished, shut down Backtrack.

- Reboot

Importante!!! Tamto para Backtrack y Kali

User: root

Password: toor



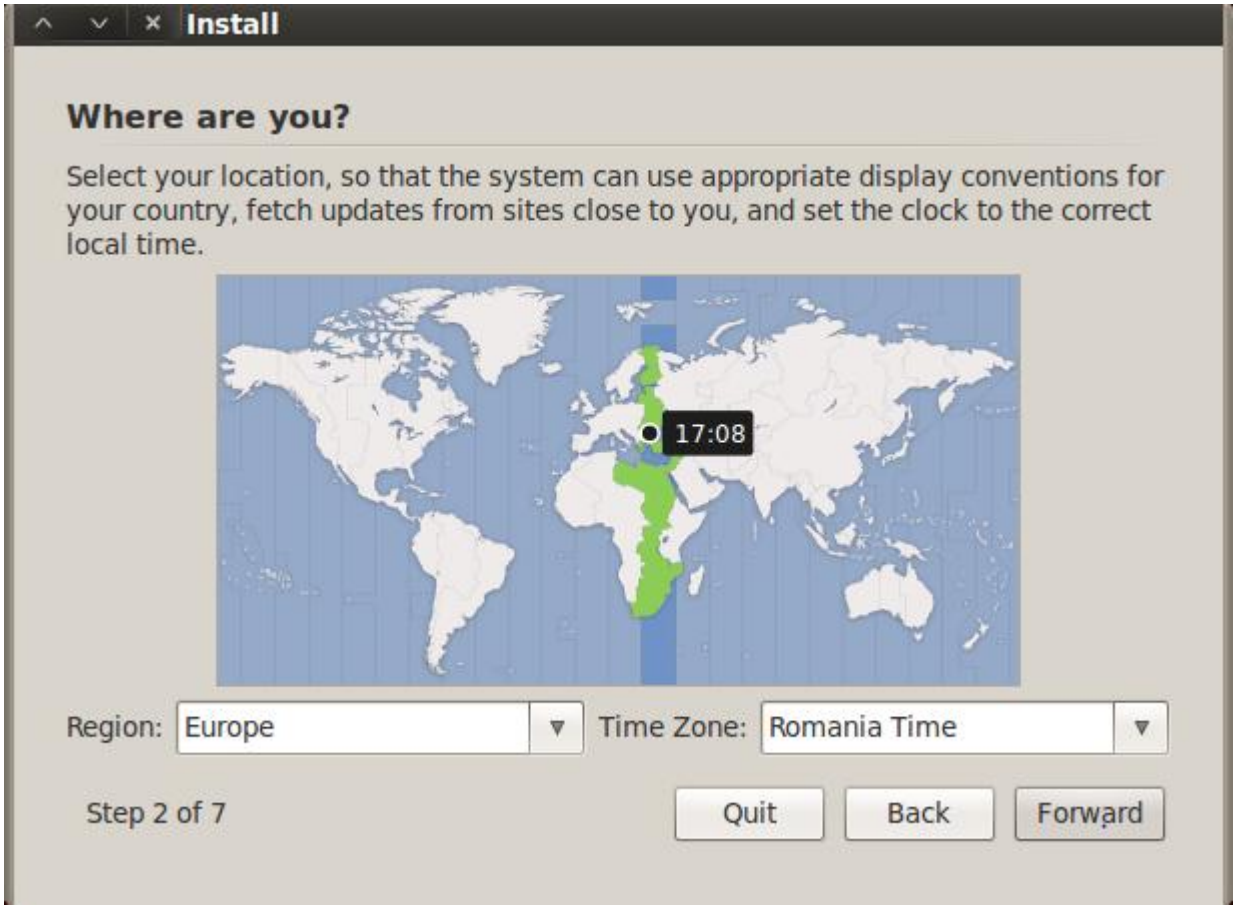
Instalar backtrack/Kali al disco de la maquina virtual

NOTE: It is recommended that you have a minimum of 20 GB free disk space to install Backtrack!

- Boot the Backtrack Live Environment.
- At the bash prompt, type **startx** to enter the GUI.
- Double click the **Install Backtrack.sh** on the desktop
- Let's run through the installer step by step:

- We select our language, in this case English and then click the **Forward** button.

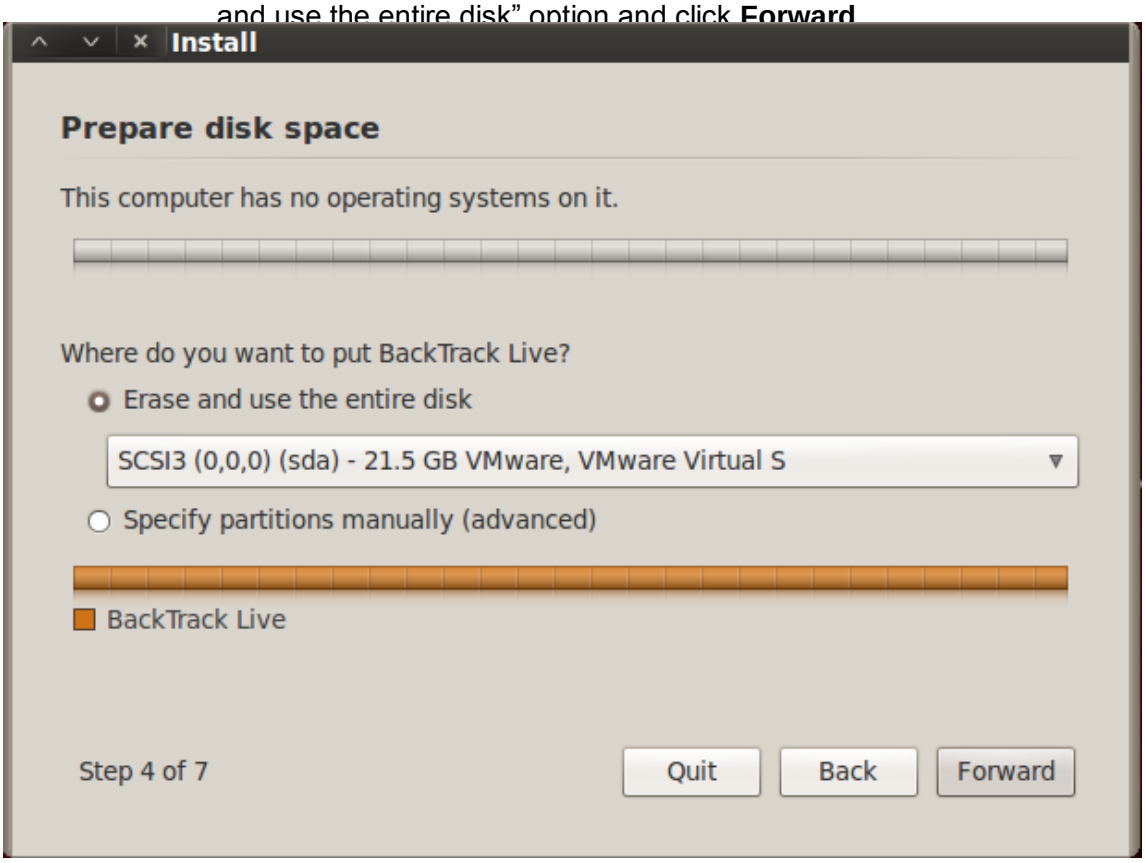
- Here we select out geographical location (The Region and Time Zone) and click **Forward**.



- Chose your keyboard layout. We are going to leave it the default which is USA and click **Forward**.

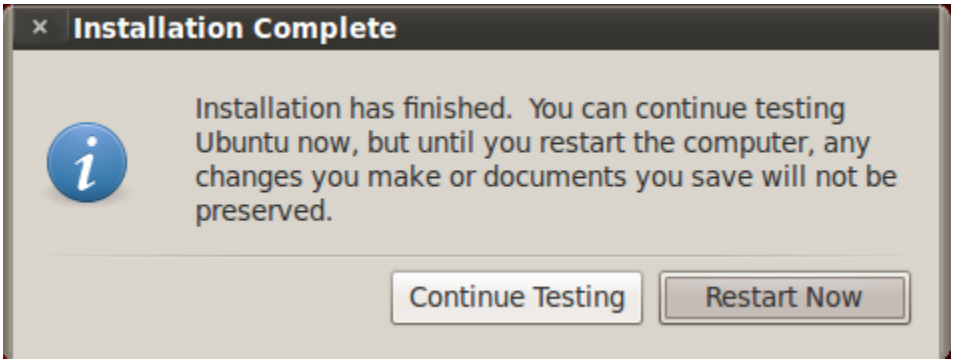

Install
Keyboard layout
Which layout is most similar to your keyboard?
Suggested option:
USA
Guess keymap:
Guess...
Choose your own:
Turkey
Turkmenistan
USA
Ukraine
United Kingdom
USA
USA - Alternative international (form
USA - Cherokee
USA - Classic Dvorak
USA - Colemak
You can type into this box to test your new keyboard layout.
Step 3 of 7
Quit
Back
Forward

- Now it's time to partition the Disk, for a full Disk installation we choose the "Erase and use the entire disk" option and click **Forward**



WARNING: Sometimes the installer will get stuck at difference percentages, leave it for a while as it will move on.

- Hit the **Restart Now** button, and enjoy Backtrack!



- After the reboot, you can log in with the default username root and password toor.
- Do not forget to change this default root password by issuing the passwd command.
- As you can see the splash screen disappeared after the reboot. In order to fix it just run fix-splash, and the splash screen will appear on the next boot.