

Recursos para taller de reconocimiento y explotación.

VirtualBox:

Antes de comenzar el taller de enumeración, reconocimiento y explotación de servicios, será necesario, disponer de una serie de entornos virtualizados para trabajar sobre ellos.

El primero de ellos, se trata de VirtualBox, un virtualizador de sistemas operativos, que nos permitirá tener diferentes sistemas corriendo a la vez en una misma máquina, para simular un entorno de trabajo. Esto será denominado Laboratorio, y en esta ocasión estará compuesto por:

- Sistema Operativo Kali Linux.
- Iso con diferentes vulnerabilidades (Debian)

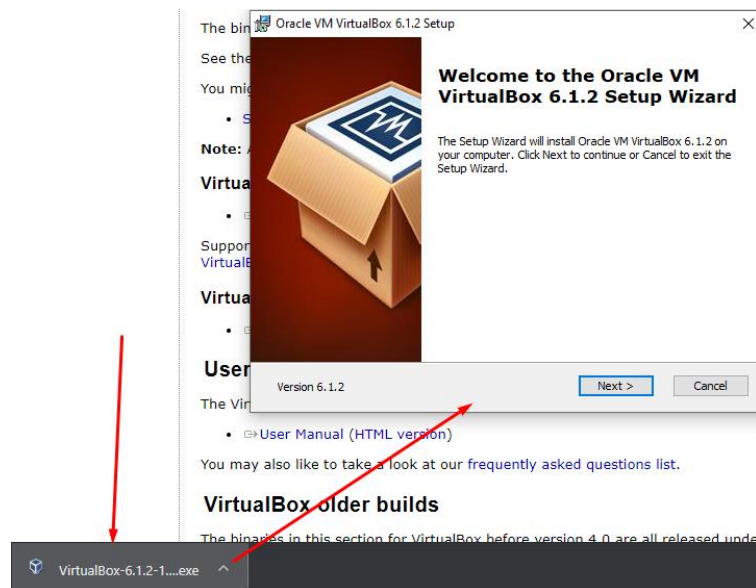
Para ello, lo primero será acceder al enlace de descarga oficial:

<https://www.virtualbox.org/wiki/Downloads>



En esta página elegiremos nuestro sistema operativo, por lo general, será windows, clickando en su correspondiente enlace, comenzando la descarga.

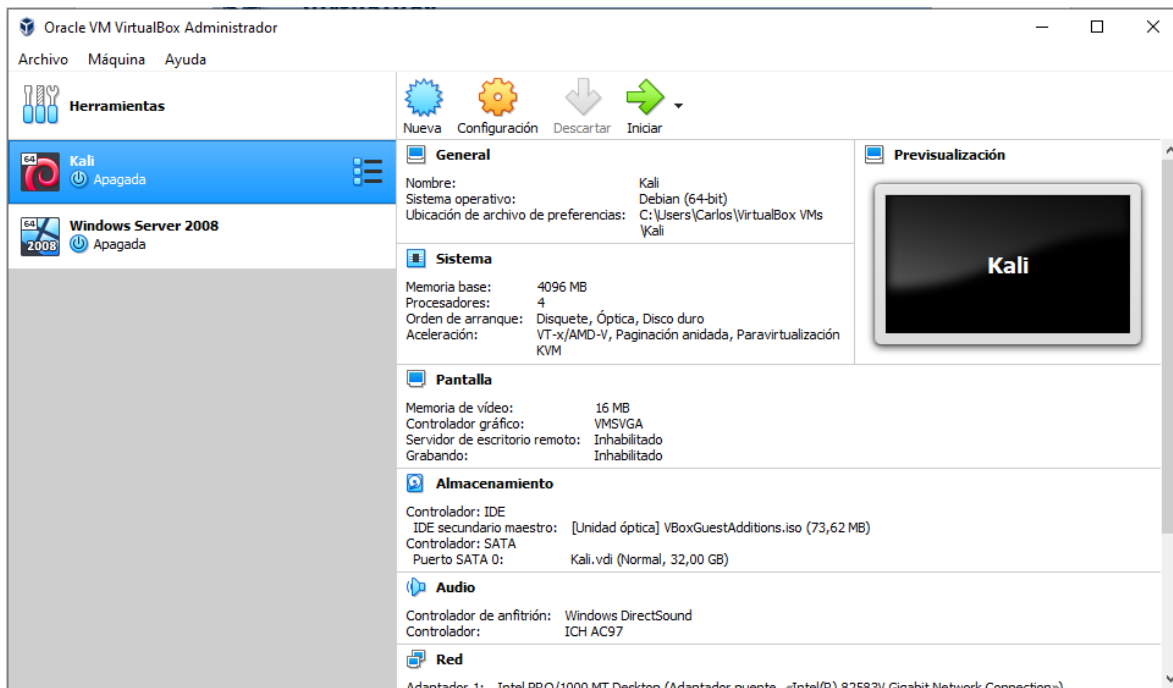
Una vez descargado, clicaremos en el ejecutable y comenzará la instalación.



Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.

La instalación de este recurso es muy sencilla, bastará con darle next todo el rato, y esperar a que finalice la barra de estado, una vez instalado obtendremos algo similar a esto:



En la columna izquierda se muestran las máquinas que tenemos instaladas actualmente, es normal, que tras la primera instalación esta columna este vacía, pero la iremos rellenando mas adelante.

Una vez hemos concluido la instalación de VirtualBox, podemos comenzar a instalar nuestro sistema operativo para realizar las explotaciones: Kali Linux.

Recursos para taller de reconocimiento y explotación.

Kali Linux

Kali Linux se trata de una distribución de Linux orientada al pentesting, gracias a ello, podemos encontrar en ella todas las herramientas (Prácticamente) necesarias para cualquier tipo de auditoria de seguridad. Kali Linux es el mejor amigo de un Pentester :)

Para comenzar su descarga nos dirigimos a la web oficial y clickamos en el siguiente enlace:

<https://www.kali.org/downloads/>

Tras



[Blog](#)

[Downloads](#)

[Training](#)

[Documentation](#)

Kali Linux Downloads

Download Kali Linux Images

We generate fresh Kali Linux image files every few months, which we make available for download. This page provides the links to download Kali Linux in its latest official release. For a release history, check our [Kali Linux Releases](#) page. Please note: You can find unofficial, untested weekly releases at <http://cdimage.kali.org/kali-weekly/>. Downloads are **rate limited to 5 concurrent connections**.

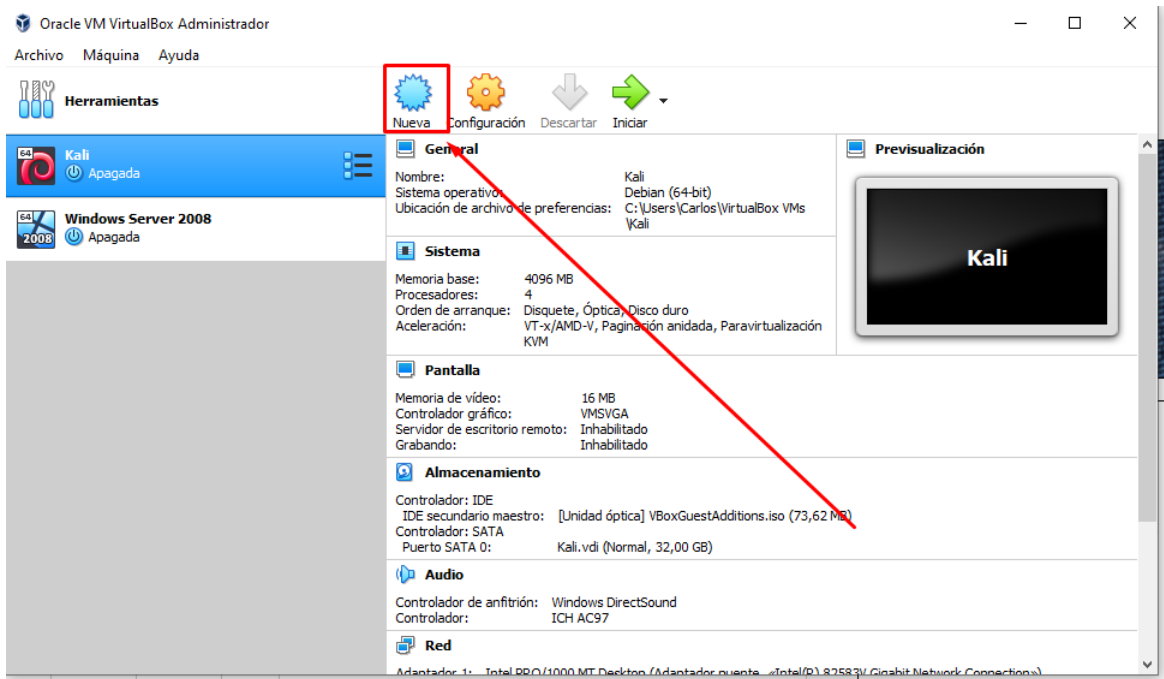
Image Name	Torrent	Version	Size	SHA256Sum
Kali Linux 64-Bit	Torrent	2019.4	2.6G	bad0d602a531b872575e23cc025b45fee475523b51378a035928b733ca395ac5
Kali Linux 32-Bit	Torrent	2019.4	2.6G	e2ad113ea0d826d8c208bd0eabd3fb4b76c7d85618d4f38b5d54d4788a5eacea
Kali Linux Light 64-Bit	Torrent	2019.4	1.2G	bb2ef76da0a56af0af068b0701ff2ba455478eb02527cf0058a148ac2f125a16

Tras clicar el enlace de descarga, obtendremos una imaan “.iso” que utilizaremos para instalar Kali Linux en nuestro Virtual Box.

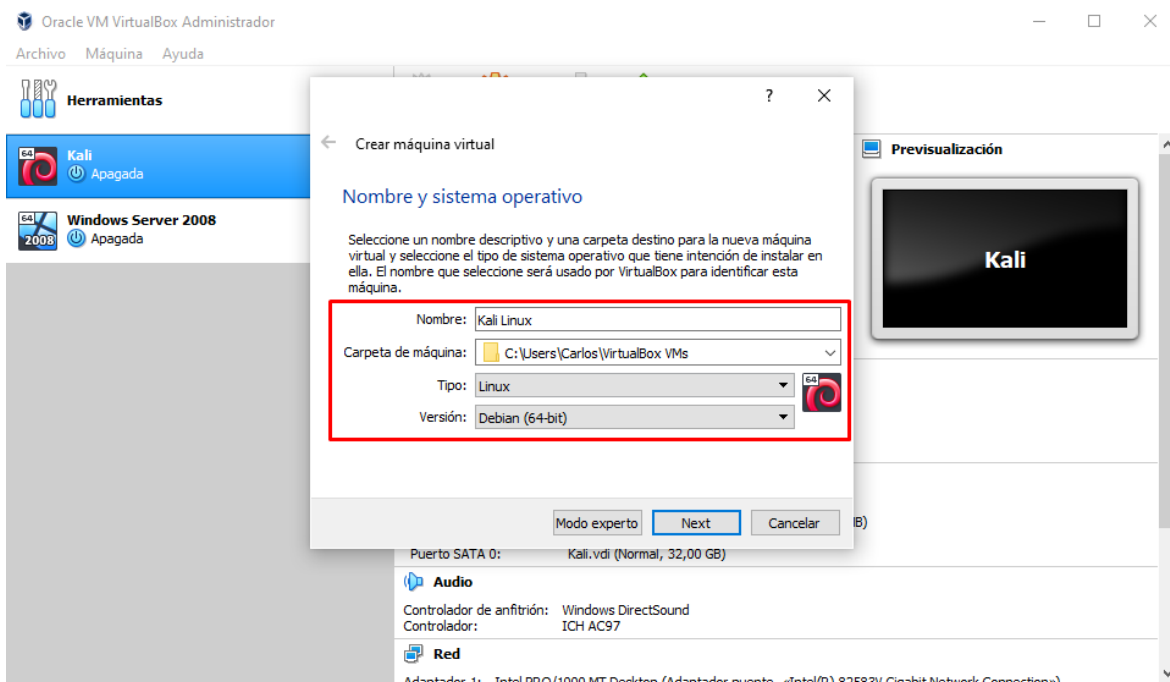
Para instalar el sistema Operativo Kali Linux sin errores en nuestro ViertualBox realizxaremos los siguientes pasos:

Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



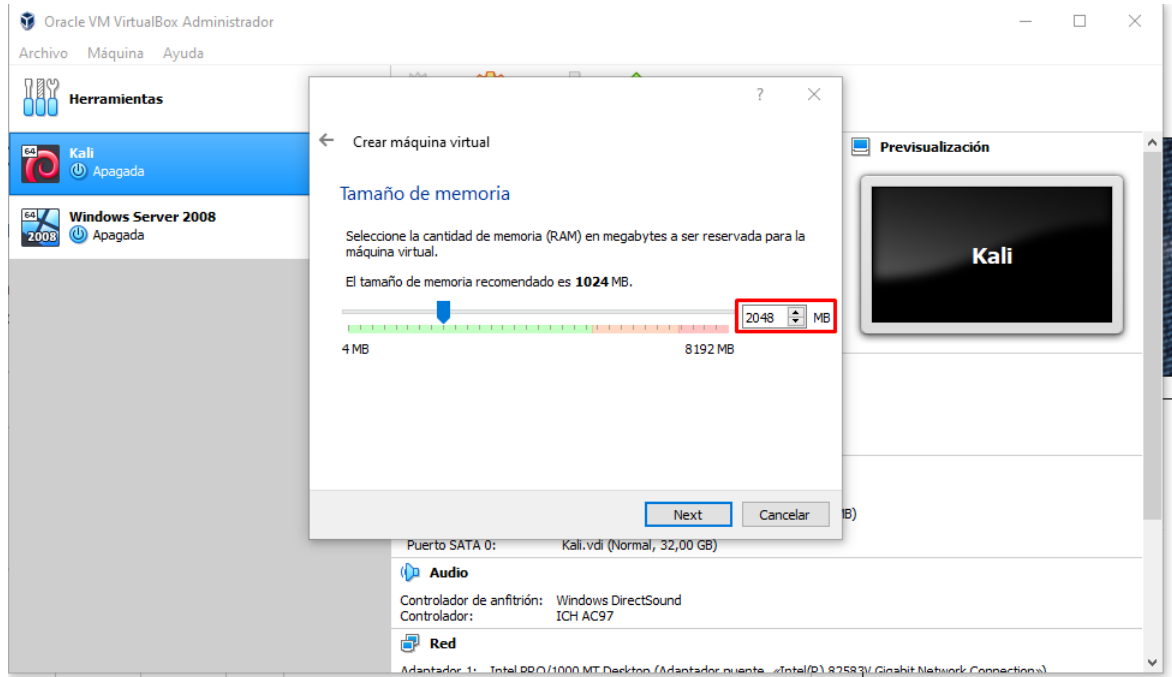
Esto abrira la siguiente pantalla:



Es muy importante en este punto, seleccionar en tipo: Linux y en Version Debian x64, asi evitamos futuros errores. Pulsamos Next.

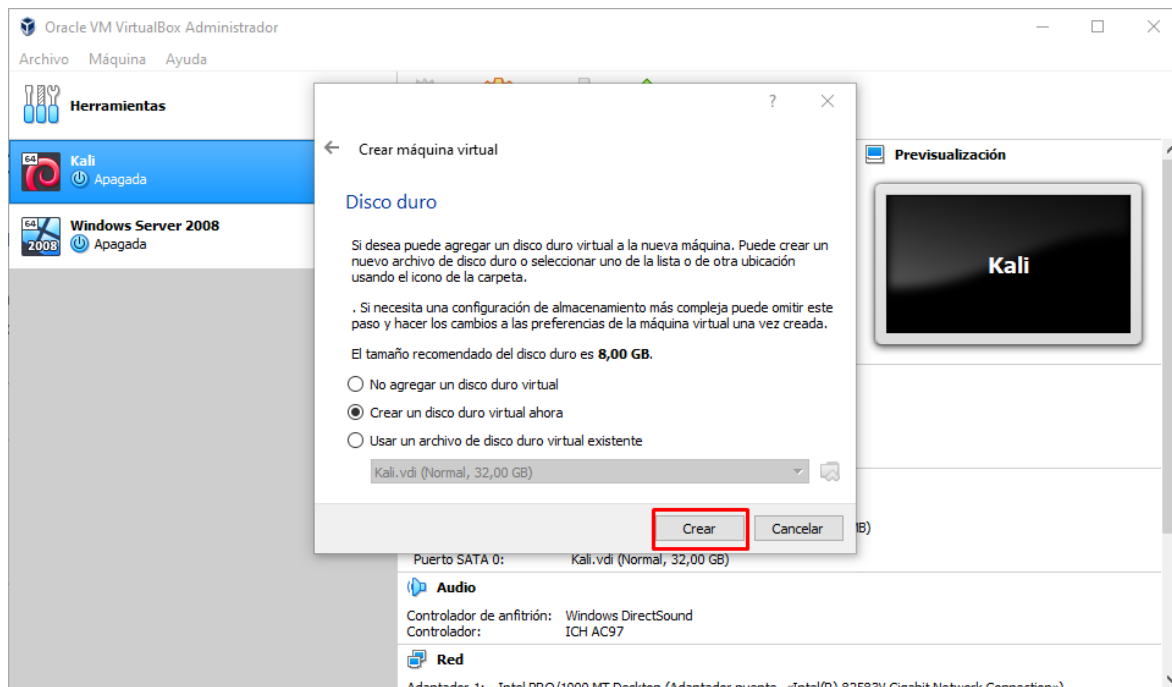
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



En la siguiente pantalla seleccionamos la RAM, en este caso MINIMO 2GB si queremos que nuestra maquina vaya minimamente fluido, esto depende de la capacidad de la maquina de cada usuario, cuanto mas RAM posea tu equipo , mas podras **NUNCA SUPERANDO MAS DEL 50%** ya que si no, la maquina anfitrión puede colapsarse.

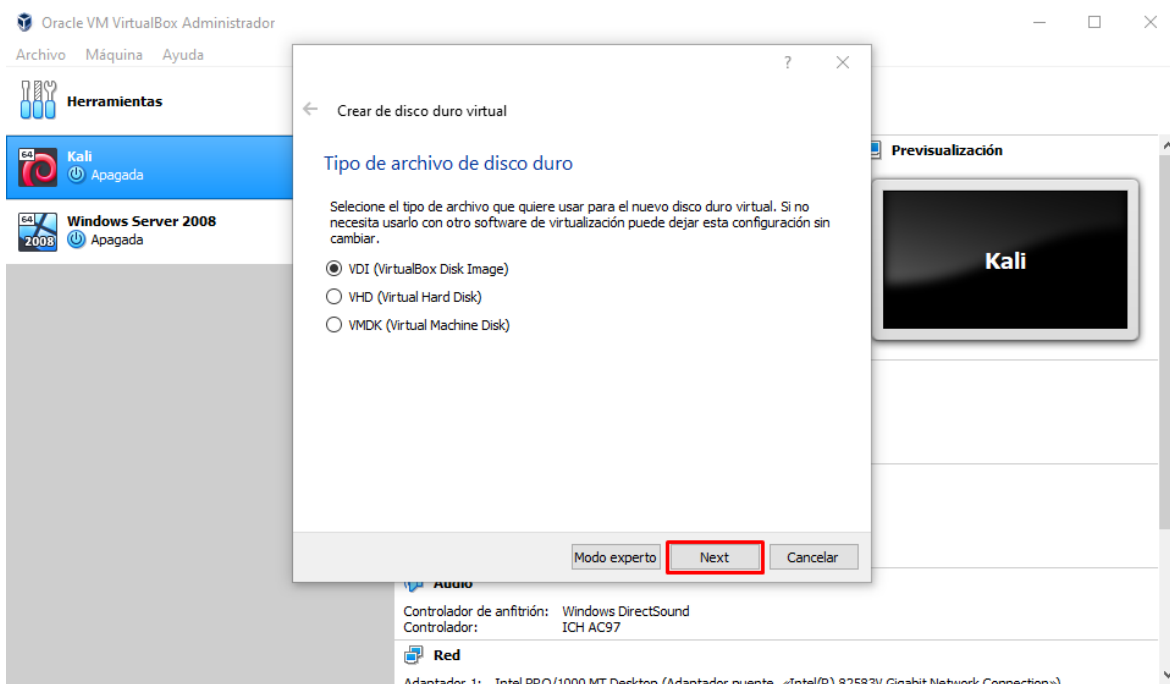
Pulsamos de nuevo Next.



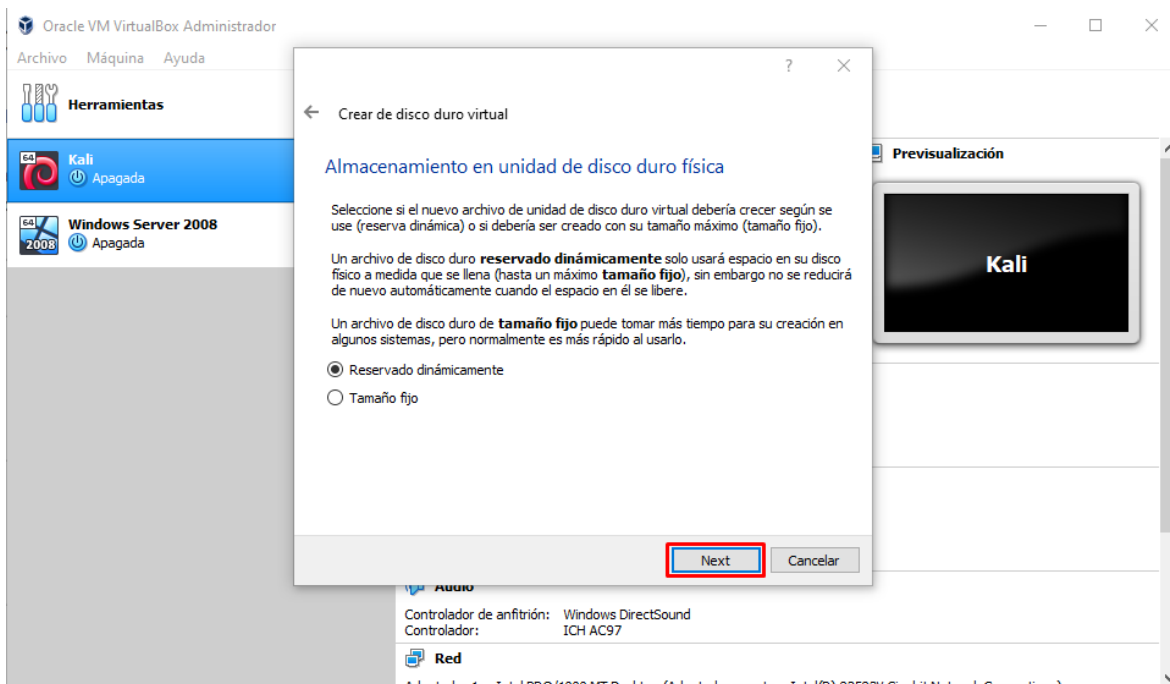
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.

Pulsamos en “Crear”.



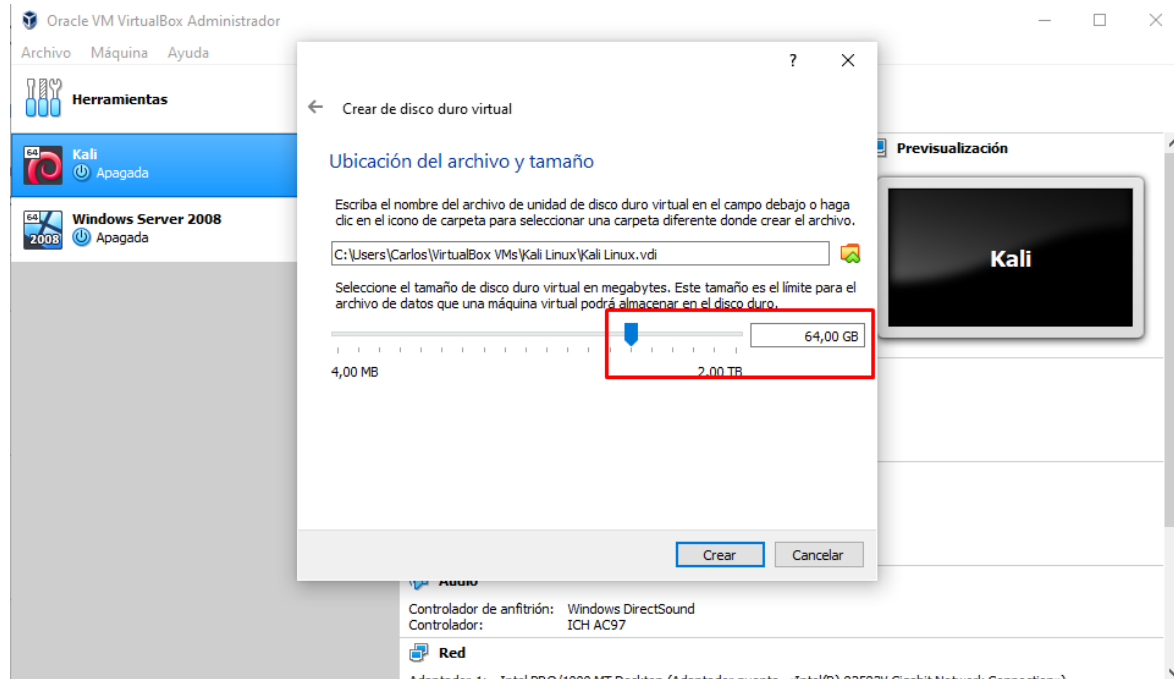
Pulsamos Next.



De nuevo Next.

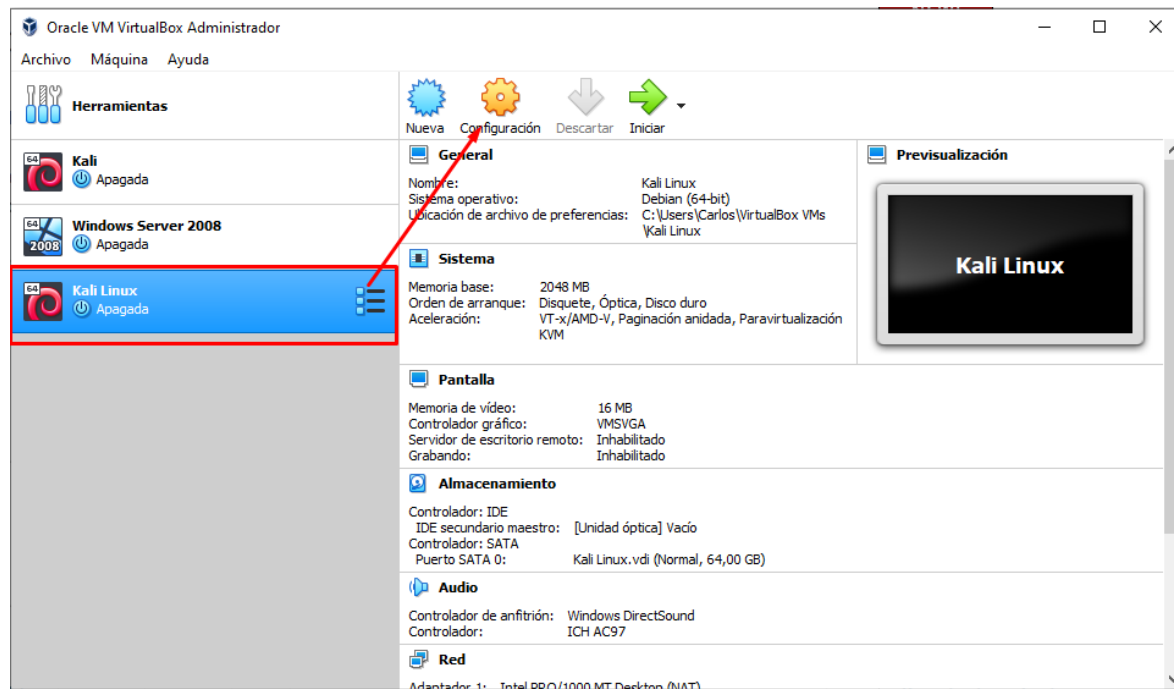
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



En la parte de establecer el tamaño de disco, es necesario saber que esta maquina la utilizaremos para unicamente este taller, por lo que no necesitaremos mucho espacio de almacenamiento, pero si esta version va a utilizarse mas adelante para realizar mas pentesting, habra que incidir un tamaño de disco grande, para no quedarse sin espacio a la hora de intalar herramientas.

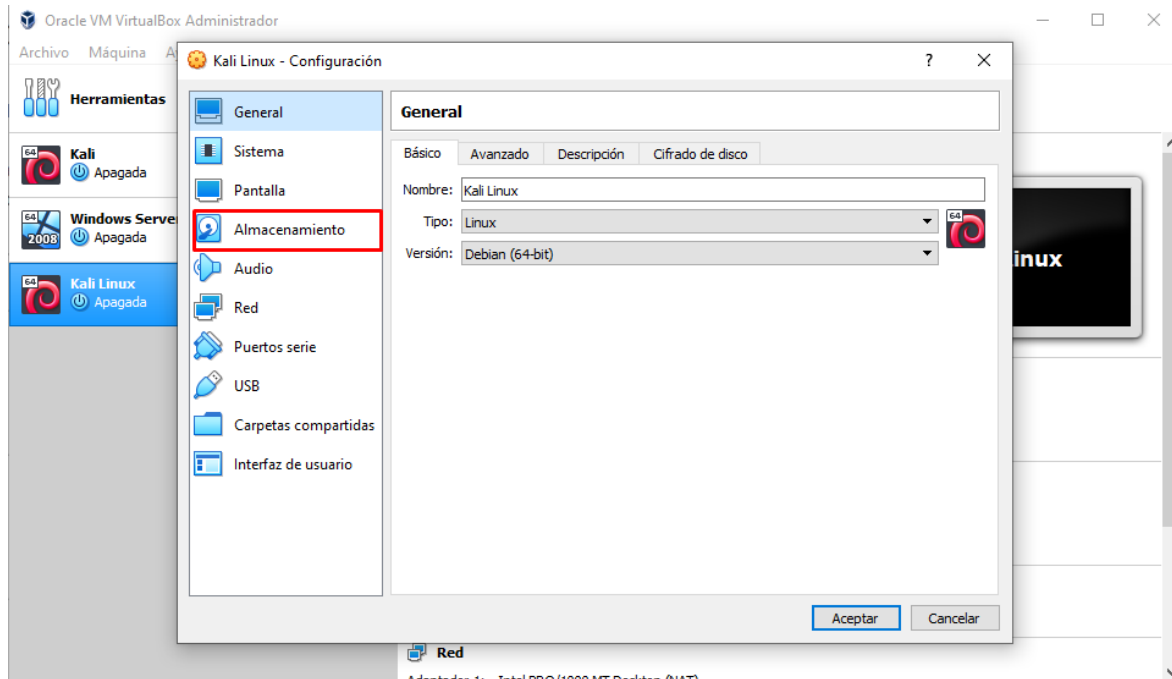
Pulsamos Crear.



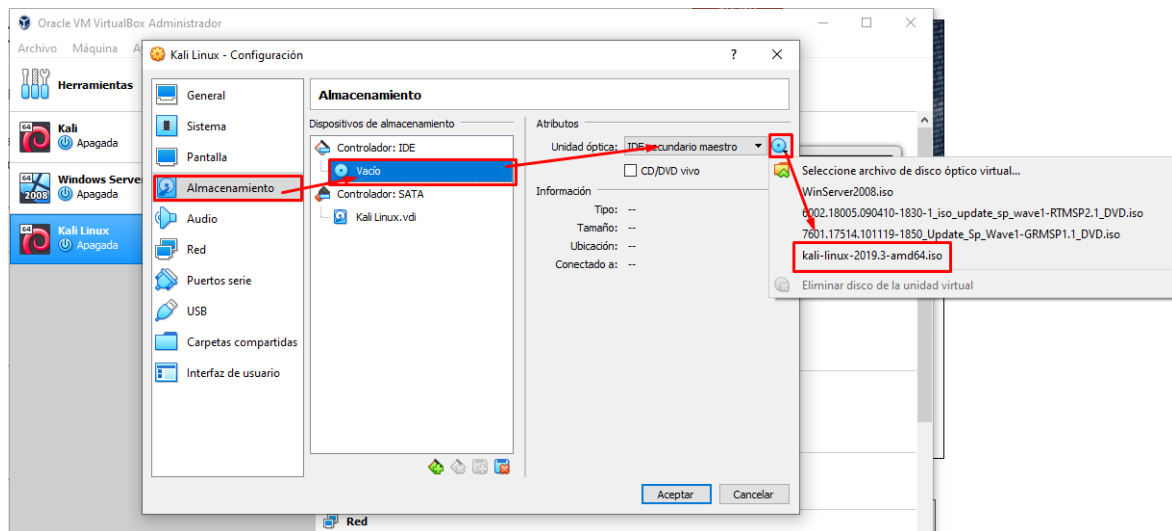
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.

Tras este proceso, ya hemos creado nuestra máquina vVirtual, que actualmente se encuentra vacía, es hora de cargar la ISO de kali que hemos descargado y comenzar su instalación, para ello nos dirigimos a Configuración.



Vamos a Almacenamiento:

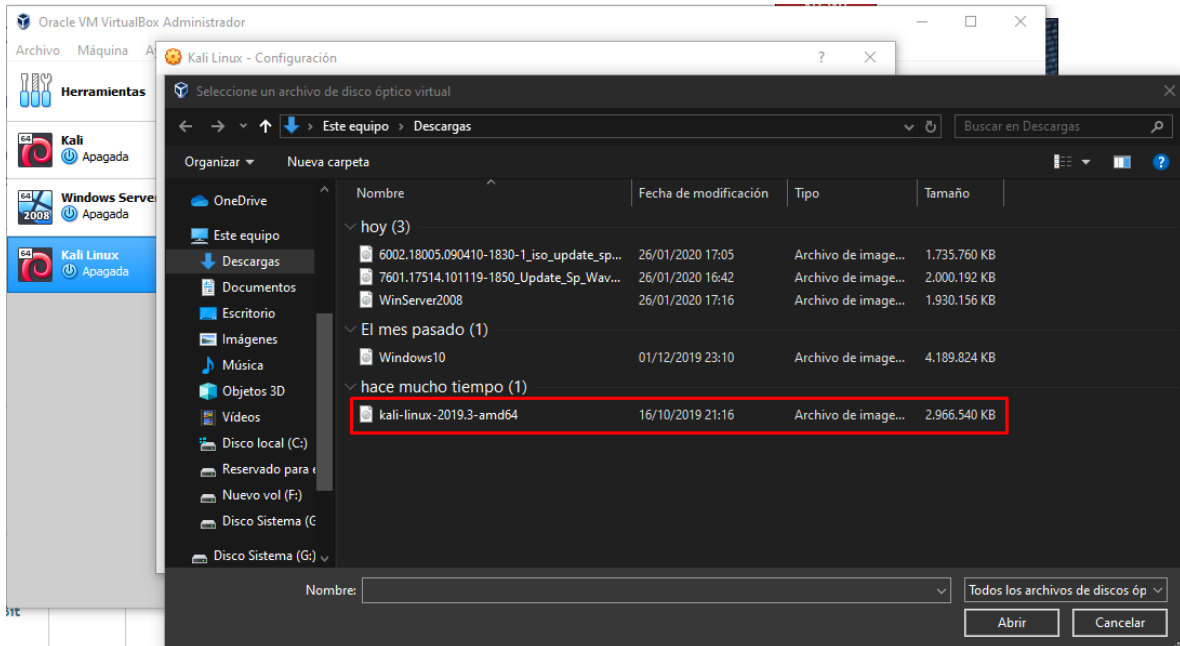


En esta pestaña, nos dirigimos al controlador IDE, y a la derecha, donde pone “Unidad Optica”, en el icono del disco, lo pulsamos y seleccionamos la imagen .iso de kali linux.

Es posible que no aparezca en el desplegable como en la imagen en ese caso, pulsamos “Seleccione un disco virtual”, abriendo esto el explorador de archivos, nos dirigimos a las descargas y la seleccionamos.

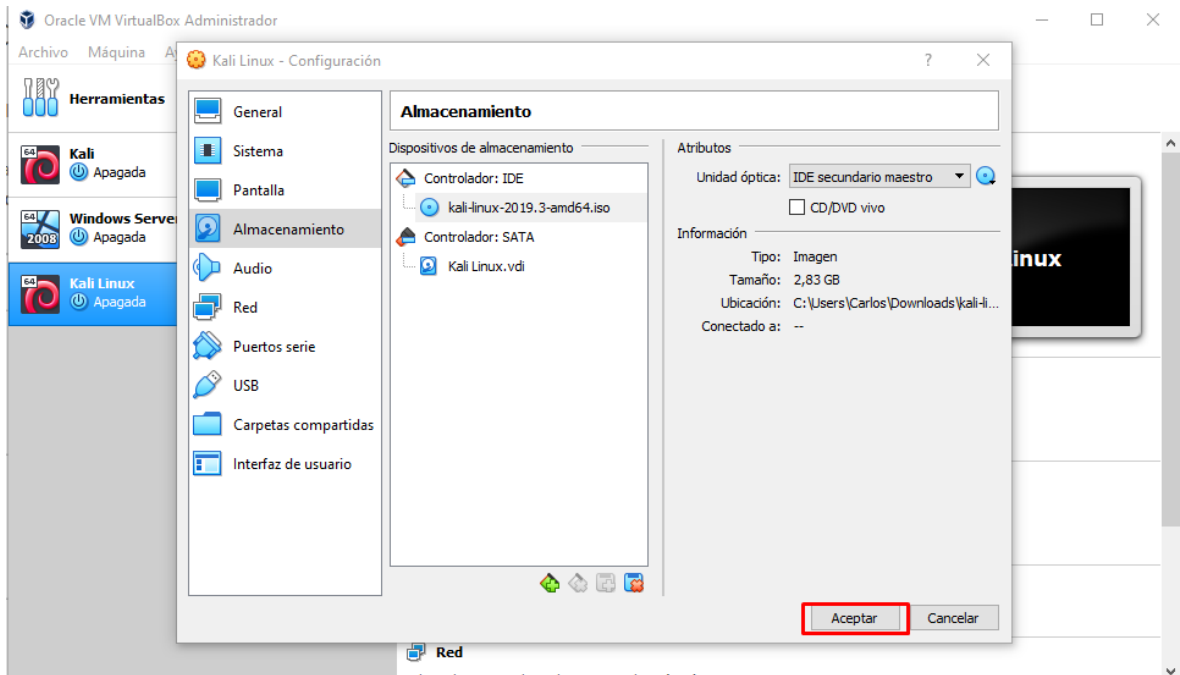
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



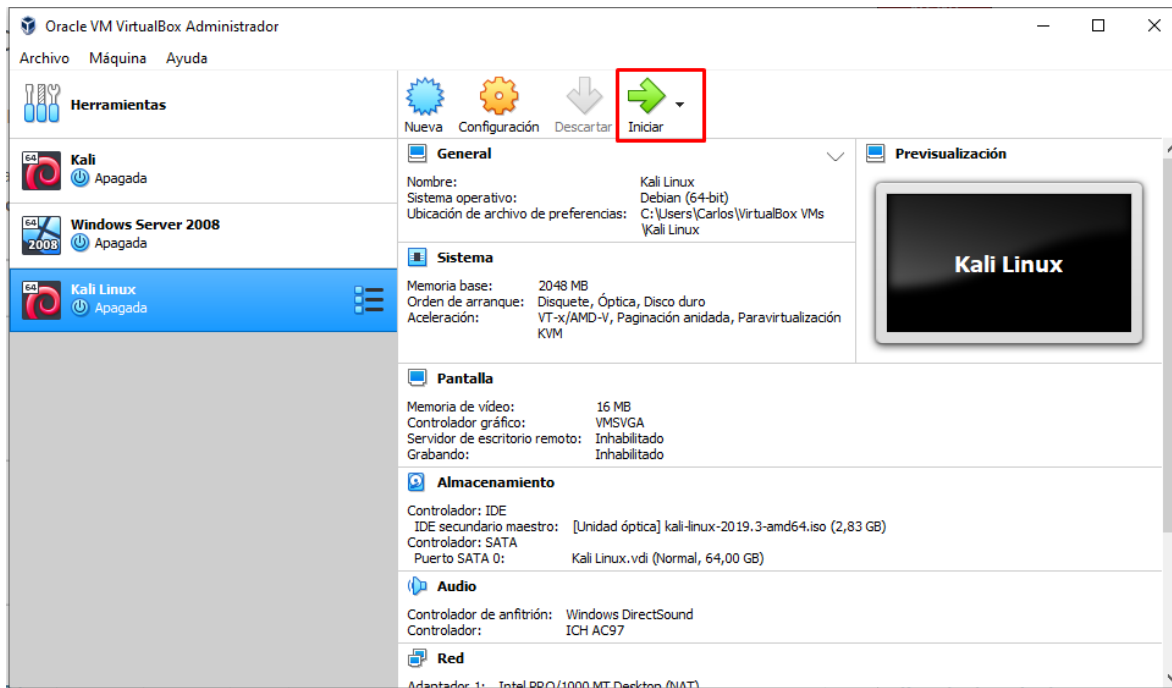
De este modo, configuramos el arranque de nuestra maquina.

Finalmente Pulsamos Aceptar y ya podemos Iniciar nuestra maquina.

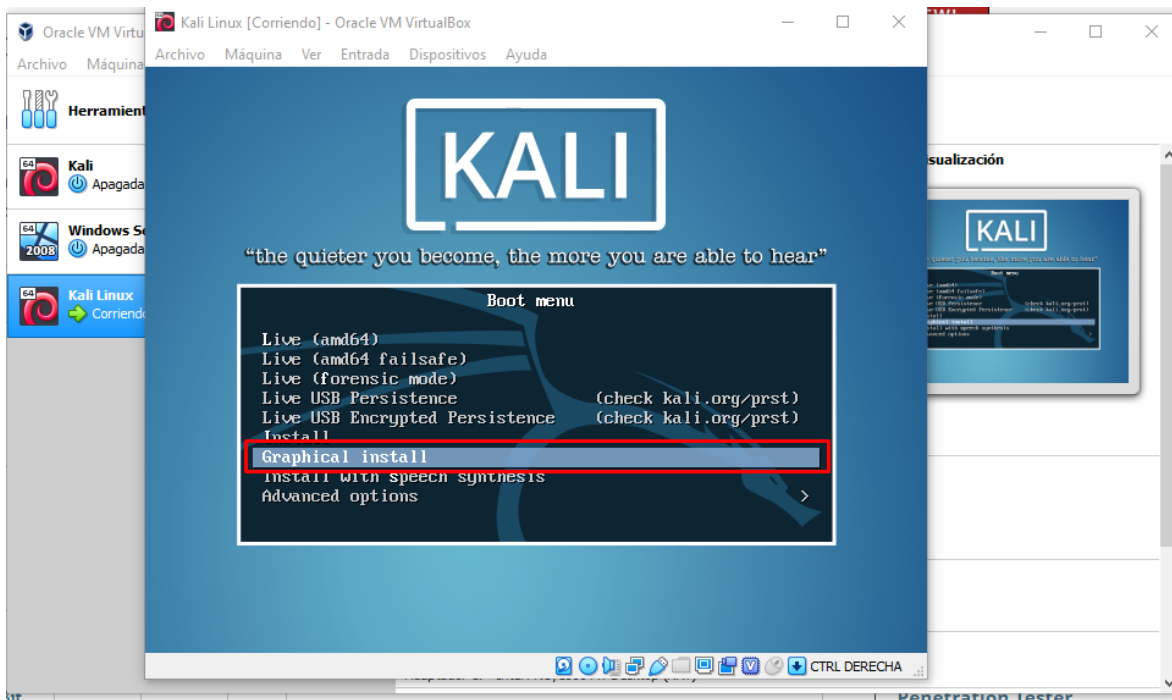


Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



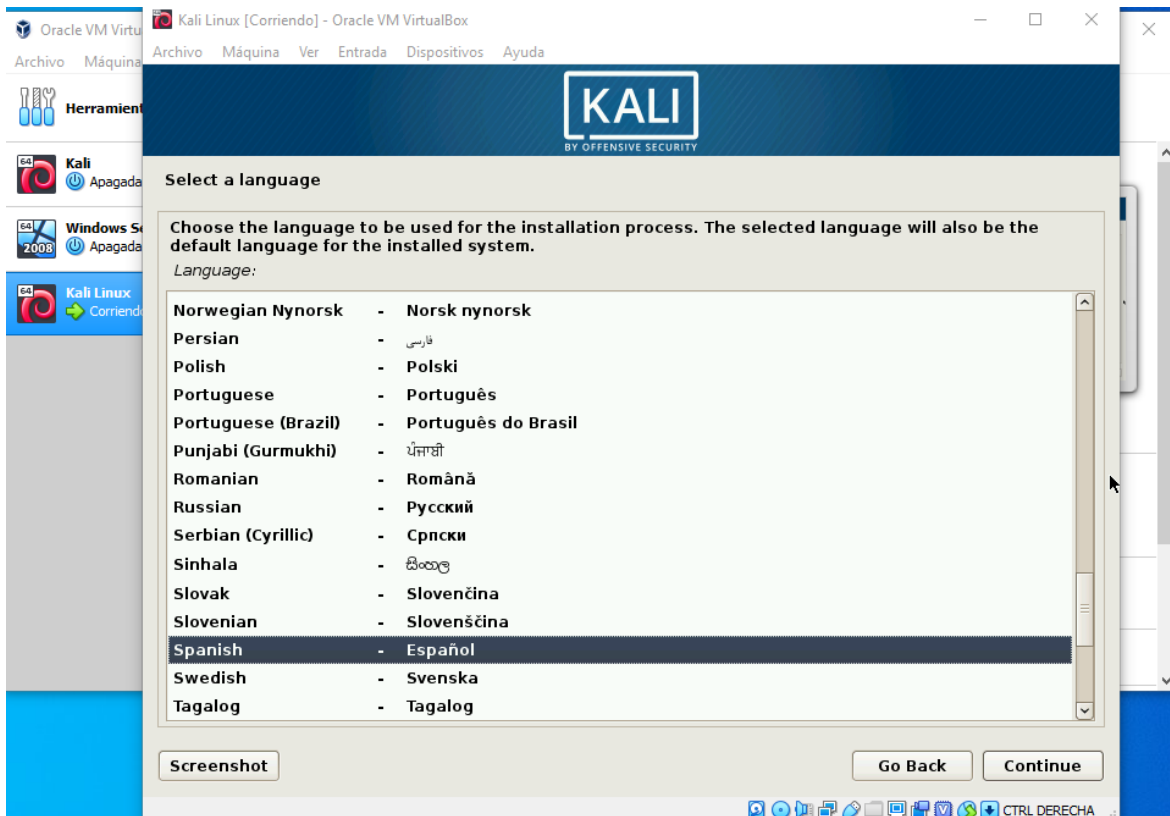
Tras iniciar la maquina comenzará la instalación del sistema operativo:



Seleccionamos Graphical Install

Realizado por: Carlos Gómez Pintado

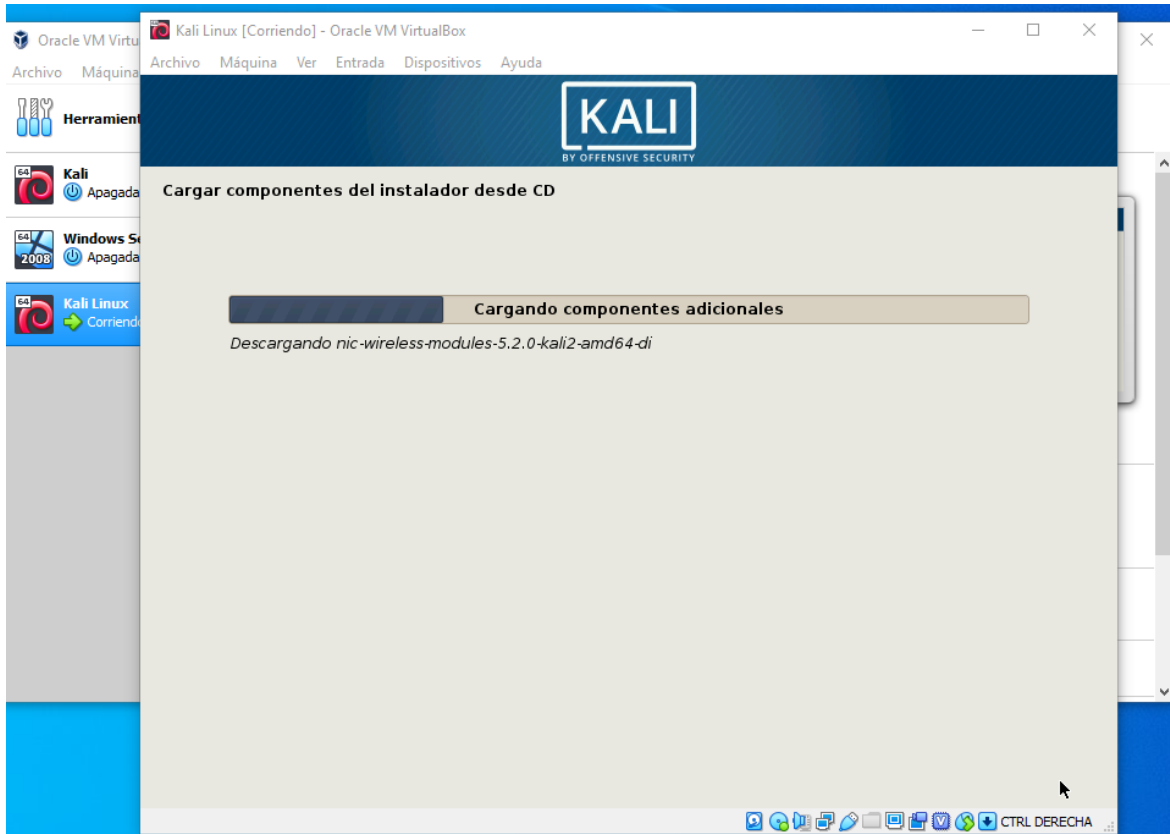
Recursos para taller de reconocimiento y explotación.



Seleccionamos el idioma, la ubicación, el teclado, y comenzara la instalacion.

Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.

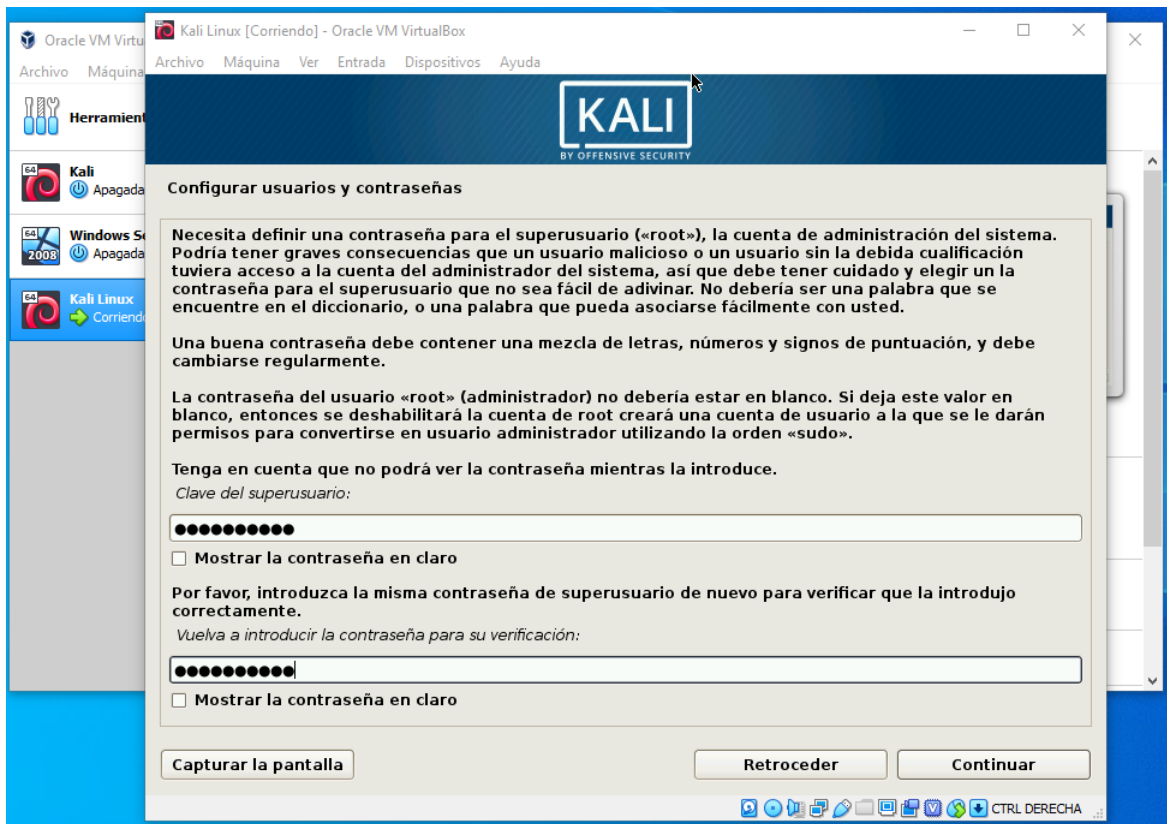


En este punto, esperamos a que termine la barra de estado, y pasamos a la siguiente pantalla, en la que seleccionaremos el nombre del equipo, yo lo dejare en Kali, pero cada cual puede seleccionar el que quiera. En nombre de Dominio, lo dejamos en blanco y le damos a continuar.

Seleccionamos la contraseña de superusuario y continuamos

Realizado por: Carlos Gómez Pintado

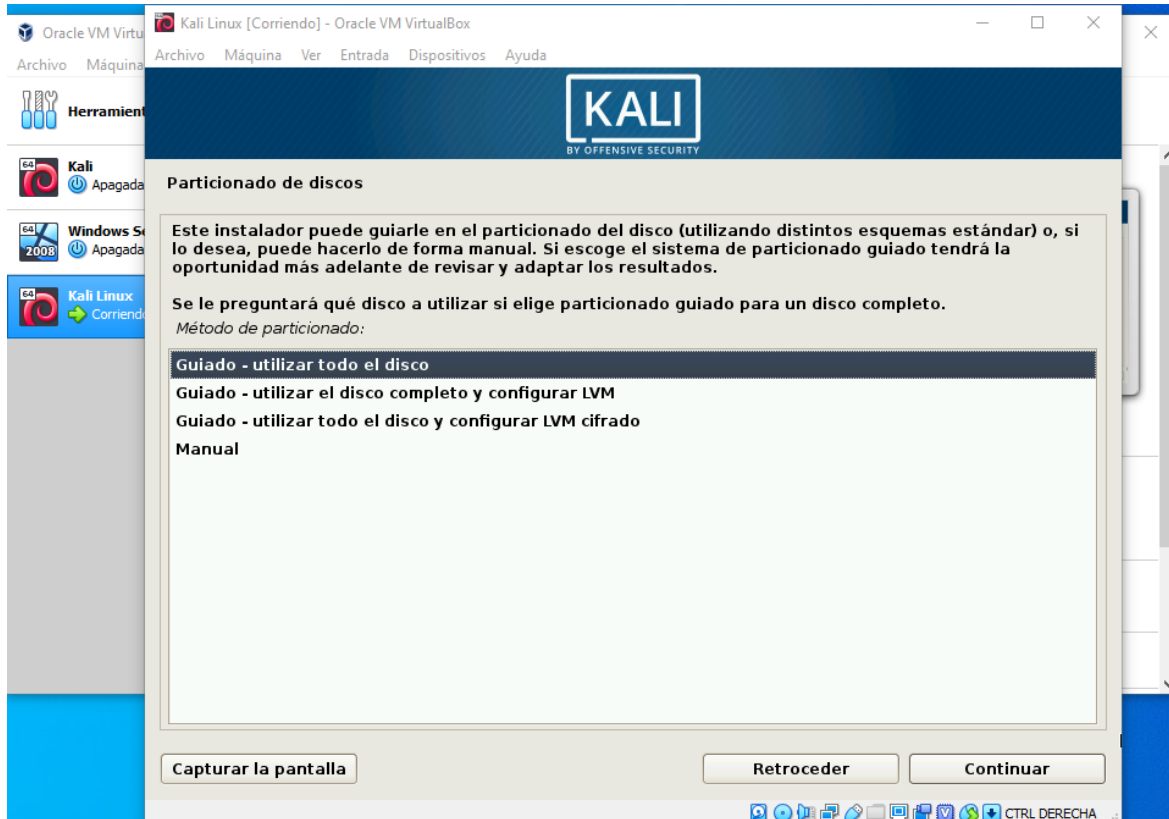
Recursos para taller de reconocimiento y explotación.



Configuramos el reloj, y procedemos a realizar el particionamiento de discos.

Realizado por: Carlos Gómez Pintado

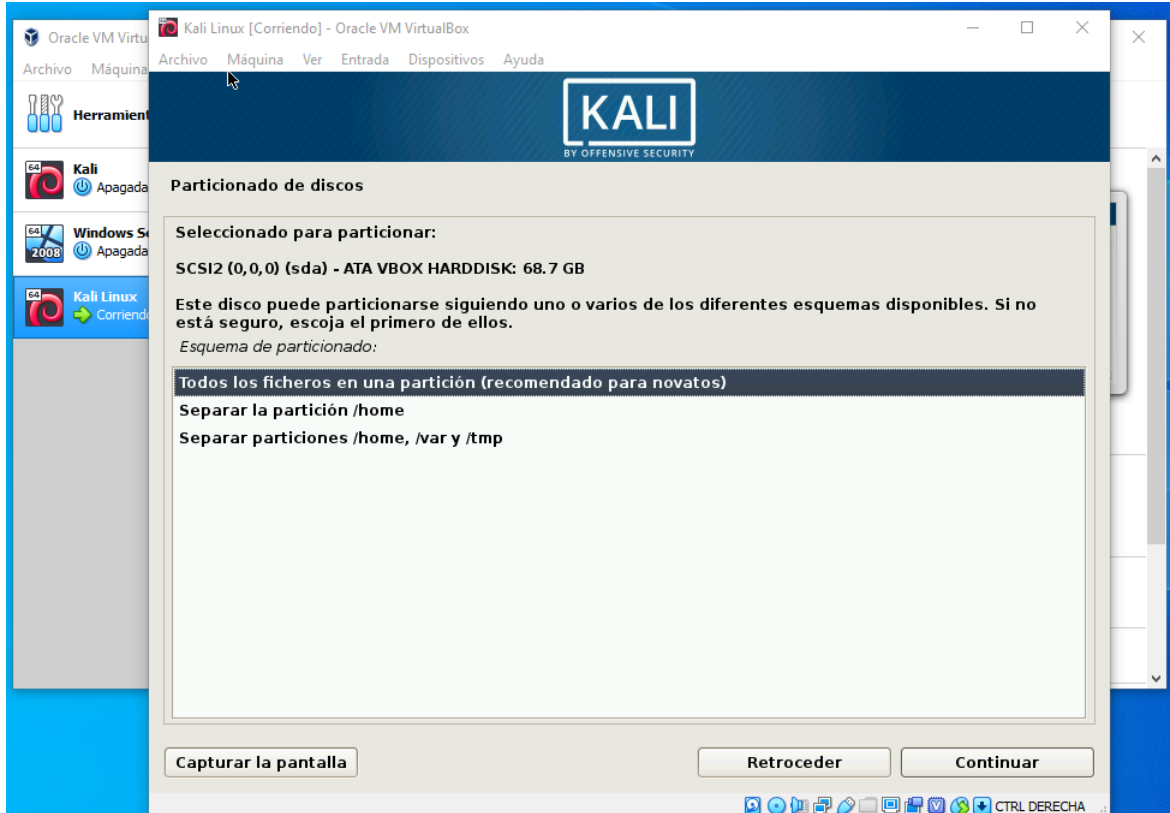
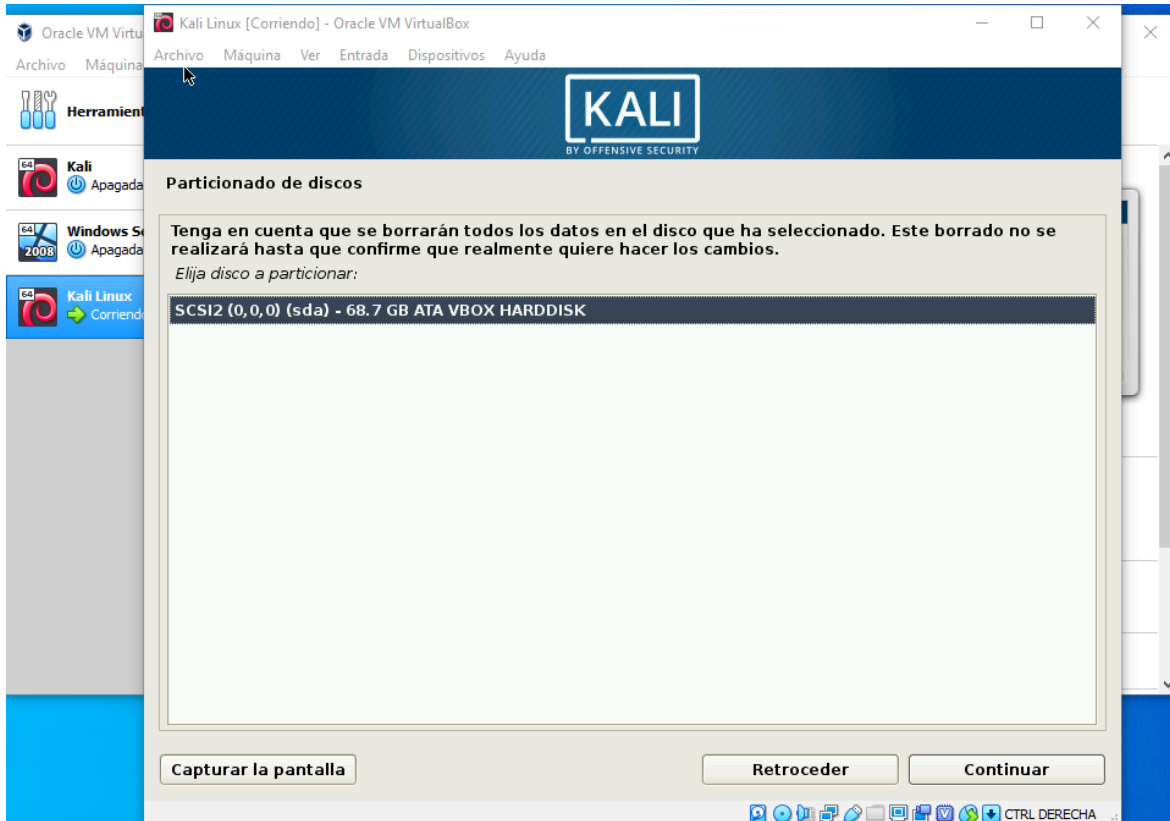
Recursos para taller de reconocimiento y explotación.



Continuamos...

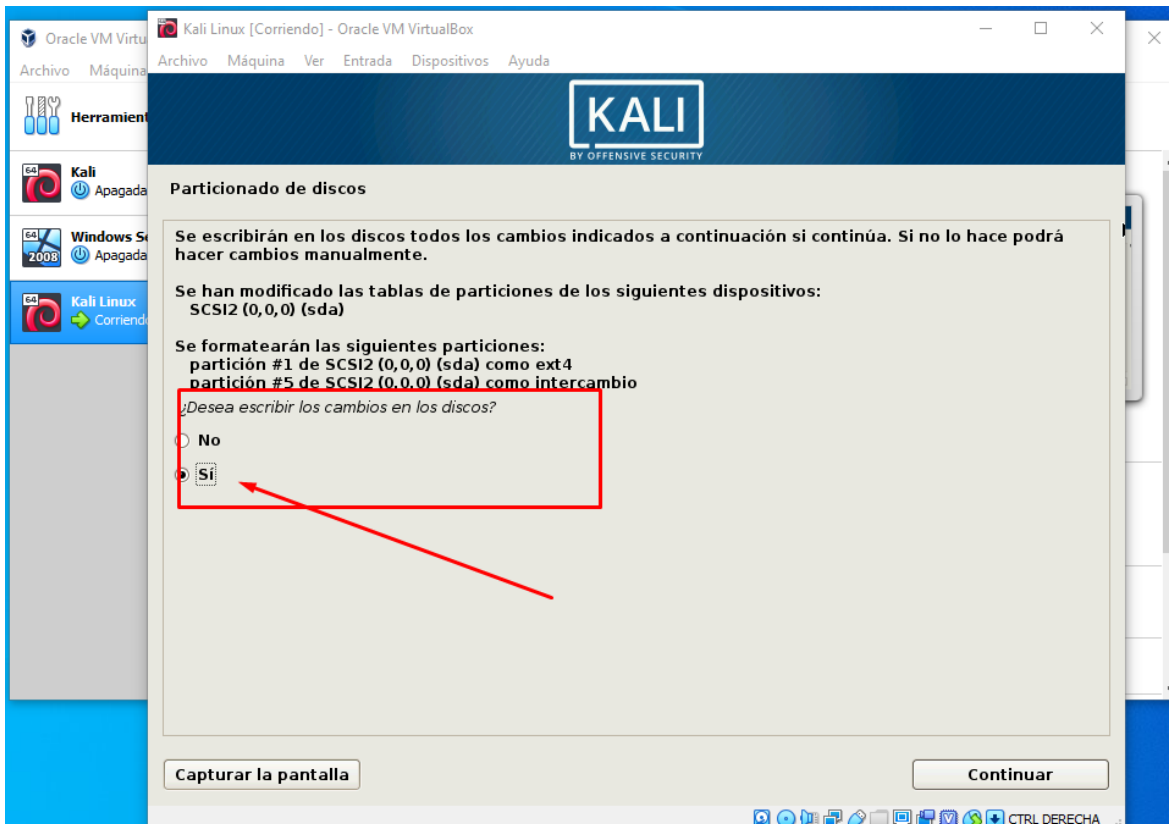
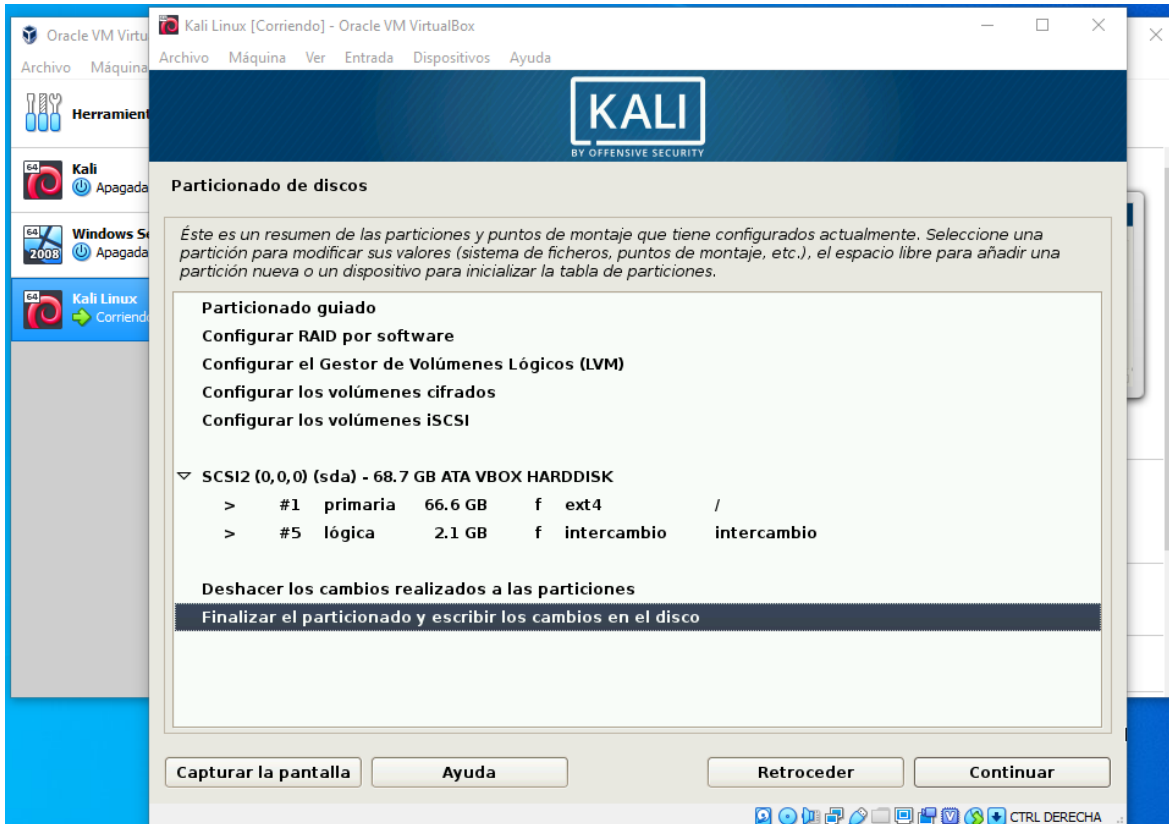
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



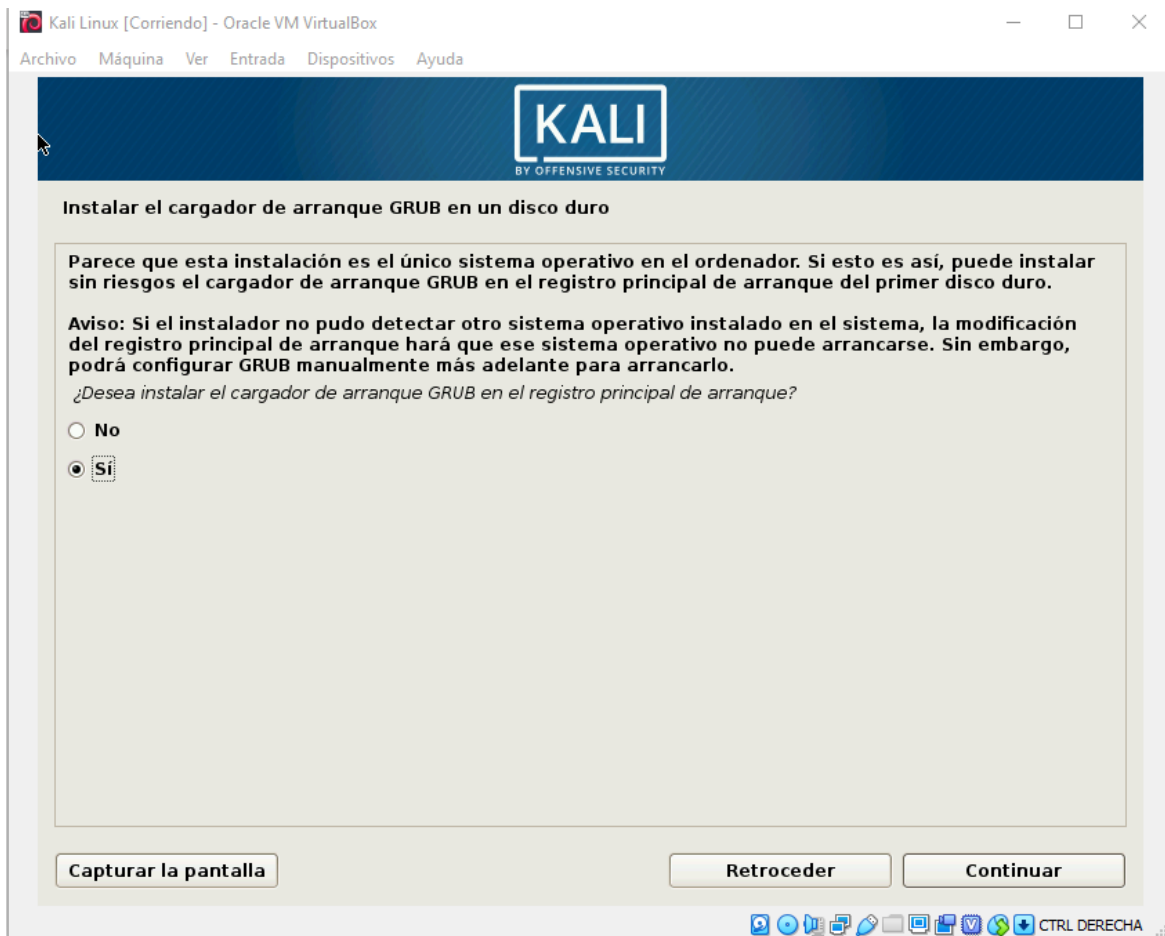
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.

Marcamos la opción de “sí” y comenzará el montaje de discos e instalación del sistema, en este punto tendremos que esperar a que se complete la información. Este proceso puede tardar un poco, así que pueden aprovechar para leer sobre Hacking :D

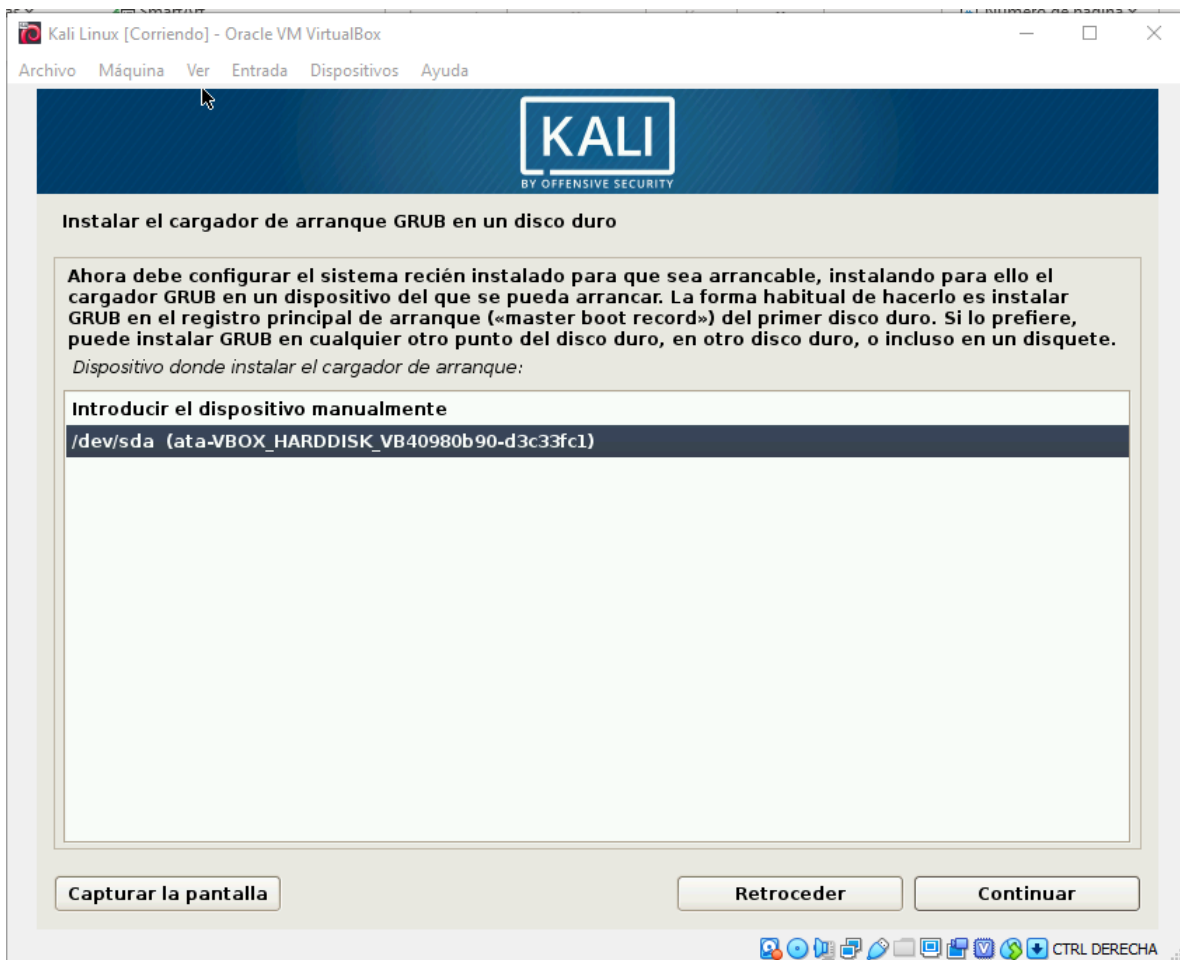
Cuando nos pregunte por la réplica de red, seleccionamos NO.

Finalmente, tan solo falta instalar el GRUB o motor de arranque, para ello seleccionamos nuestra partición de disco y le damos a continuar.



Realizado por: Carlos Gómez Pintado

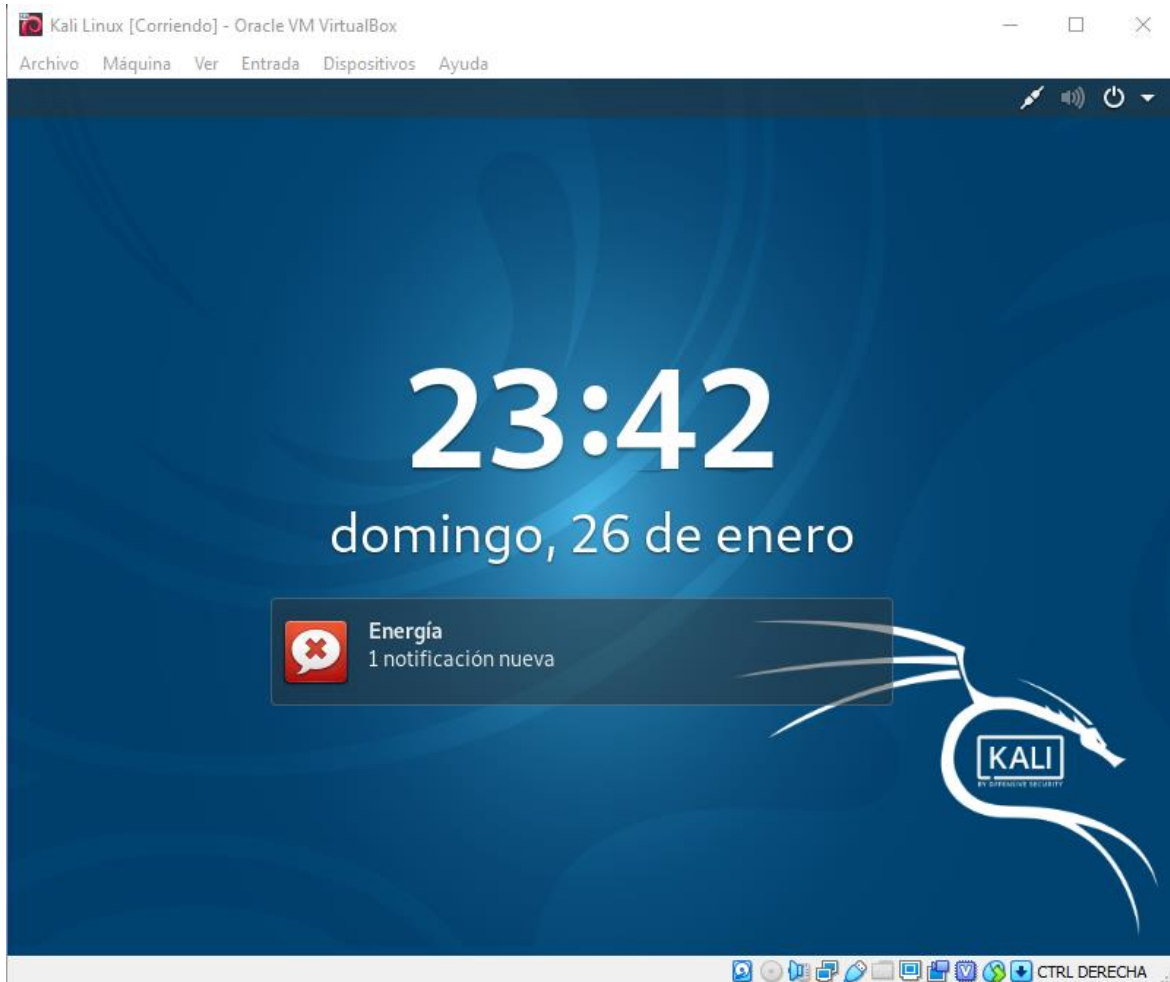
Recursos para taller de reconocimiento y explotación.



Y de esta manera terminamos la instalación de nuestro Sistema Operativo Kali Linux.

Realizado por: Carlos Gómez Pintado

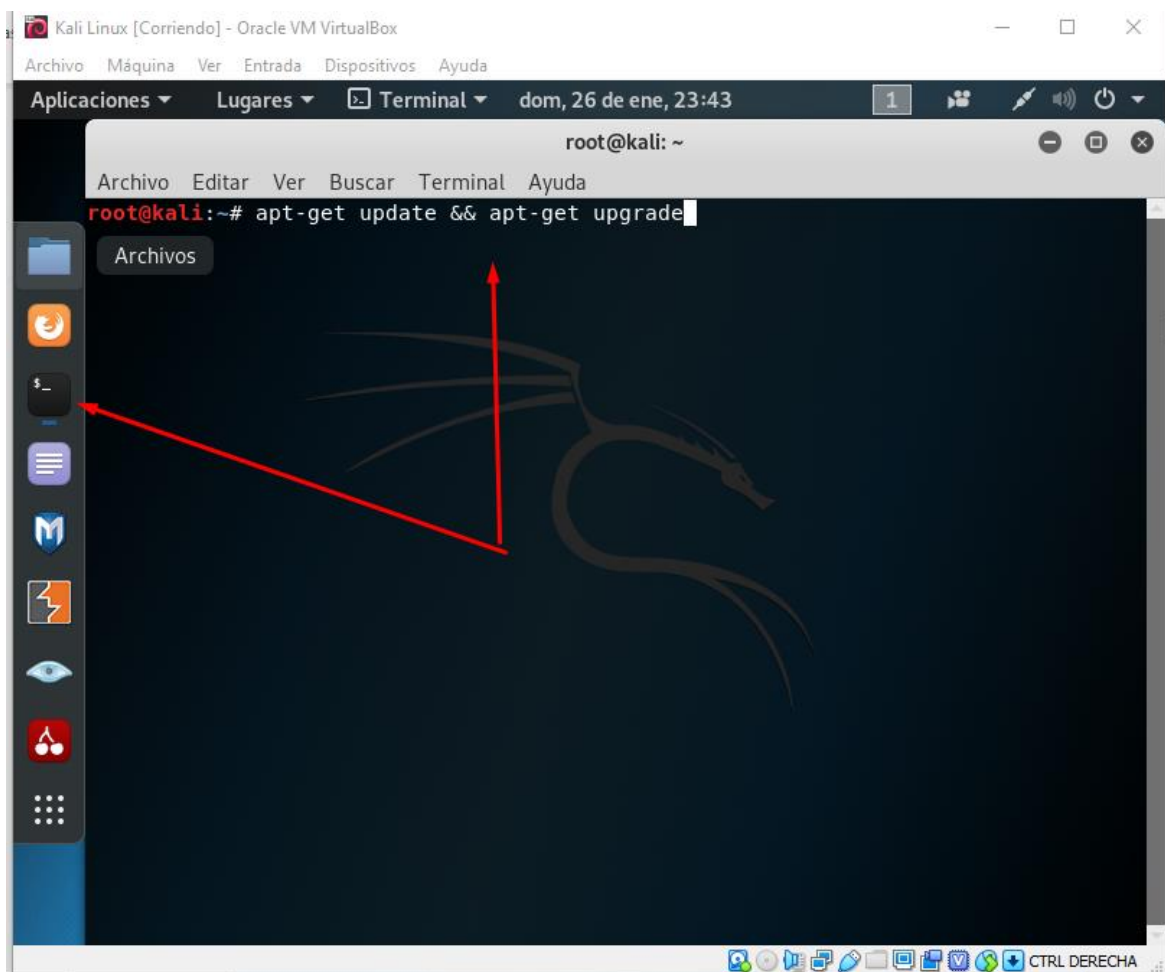
Recursos para taller de reconocimiento y explotación.



Ahora tan solo nos quedara actualizarlo, y tendremos todo loisto para comenzar a ser unos verdaderos pentesters.

Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.



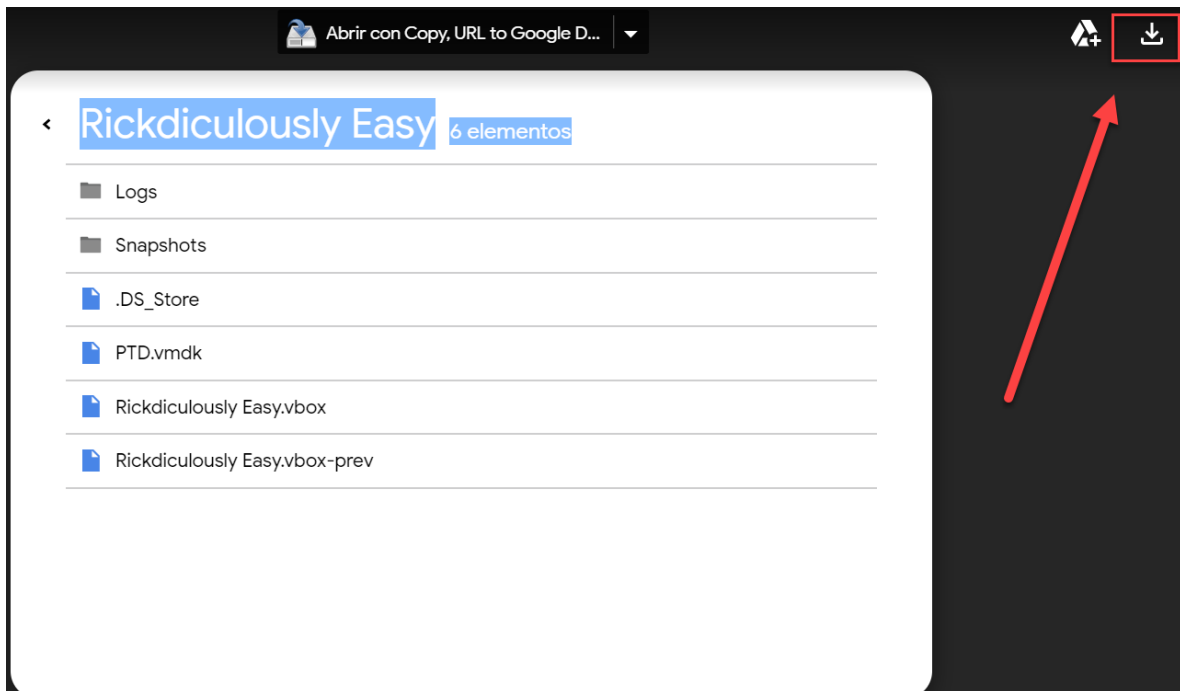
Realizado por: Carlos Gómez Pintado

Recursos para taller de reconocimiento y explotación.

Sistema Vulnerable

Para este taller vamos a utilizar una imagen de disco vulnerable, creada para ser explotada, y demostrar varias vulnerabilidades. Esta imagen, la hemos obtenido de la web “vulnhub” famosa página en el mundo del pentesting por la cantidad de imágenes con diferentes vulnerabilidades que aloja.

En este caso utilizaremos la imagen: Rickdoculously easy. Podemos obtenerla desde:



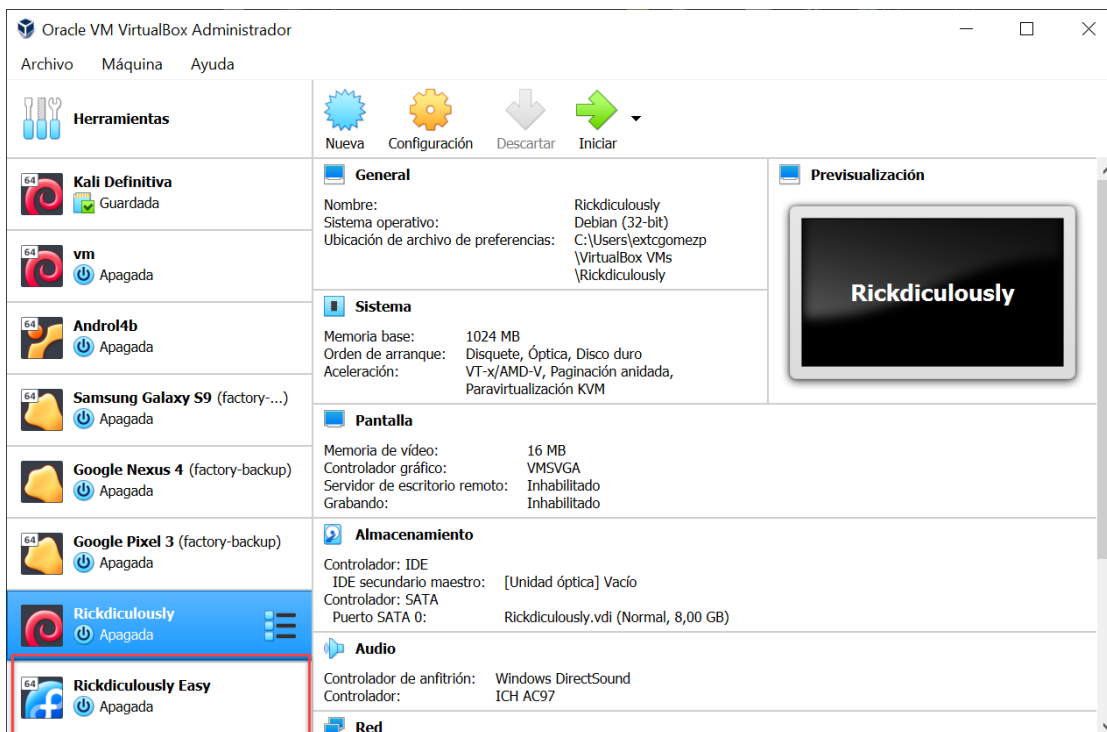
Una vez mas abrimos nuestro Virtual Box y seleccionamos la opcion de nueva:

Tras la descarga, descomprimos el archivo Zip descargado y hacemos doble click en el archivo de virtual box:

Recursos para taller de reconocimiento y explotación.

Nombre	Fecha de modificación	Tipo	Tamaño
Logs	21/09/2017 1:44	Carpeta de archivos	
Snapshots	20/08/2017 17:18	Carpeta de archivos	
.DS_Store	25/08/2017 6:46	Archivo DS_STORE	
PTD	21/09/2017 2:31	Virtual Machine Disk	2.079.4
Rickdiculously Easy	21/09/2017 11:38	VirtualBox Machine D...	
Rickdiculously Easy.vbox-prev	21/09/2017 2:31	Archivo VBOX-PREV	

Unicamente haciendo doble click, se instalara y añadira automaticamente a nuestro virtual box.



Con esto ya tendremos montado nuestro laboratorio, a falta de unos pequeños retoques finales.

Happy Hacking :)

Realizado por: Carlos Gómez Pintado