

# Pentesting con Kali Linux

Tutor: **MagoAstral**

Taller de Pentesting con Kali Linux

Introducción

Conf. VM

VMWARE



XFCE

Repositorios

Actualizar  
Kali

Instalación  
en una VM

Update  
Upgrade

**UNDERCODE**

**Eres libre de copiar, distribuir y compartir este material  
respetando la fuente y autor**

# INTRODUCCIÓN

Estimado lector le damos la bienvenida a esta nueva edición en la saga Pentesting del foro Underc0de, yo soy MagoAstral y me complace ser el tutor que desarrollará esta edición. Al igual que usted soy un aficionado a la seguridad e inseguridad informática y veo muy oportuna la creación de un manual hablando un poco de esa caja de herramientas que suele utilizar el pentester en sus auditorías, y qué mejor momento que con la salida de la nueva versión de Kali Linux.

He de decir que se tratará de una instalación desde la perspectiva de un usuario novato. Antes de comenzar con la temática, **enumeraré los requisitos** para poder llevar a cabo las fases que se desarrollarán en este taller o manual:

- **Un software de virtualización que en esta ocasión se utilizará VMware Workstation 11**
- **Imagen de Kali Linux versión 2.0**
- **10 GB libres para la instalación del sistema**
- **768 MB de RAM para Gnome 3**

Estos serían los requisitos aconsejables; cabe destacar que el entorno de escritorio se cambiará a lo largo del manual a otro más liviano (xfce), este paso es por gusto y comodidad. Si usted se siente seguro con Gnome, puede seguir con Gnome, no soy nadie para incitar al uso de un entorno que desconoce, aunque sí le aconsejo probarlo.

Como sabemos a la hora de realizar un test de penetración, el tiempo es un factor que juega en nuestra contra y por consiguiente es muy importante automatizar el proceso, es por esa razón por lo que utilizamos una distribución orientada a dicho menester pues normalmente nos abastecerá de cualquier herramienta que necesitemos. Personalmente me gusta la cita: “Lo importante no es el tiempo que tienes, si no como utilizas dicho tiempo”, y es ahí donde Kali Linux entra en juego.

Antes de comenzar con la instalación vamos a hablar un poco de Kali Linux, obviamente es una distribución diseñada para la seguridad informática y las auditorías que a su vez está basada en Debian (GNU/Linux) y fue fundada por Offensive Security Ltd.

Su lanzamiento inicial fue el 13 de marzo de 2013 y se considera como el sucesor de BackTrack (los que lleven un poquito en el mundo del pentest habrán trabajado con él), la segunda versión de Kali Linux fue lanzada el 11 de agosto de 2015. Un dato importante a destacar es que Kali Linux al tener diversas herramientas para la seguridad y auditoría es recomendable correrlo bajo un superusuario (root) para evitar conflictos.

Desde mi punto de vista os recomiendo utilizarlo virtualizado y en un segmento de red aislado a la hora de auditar vuestros laboratorios pues no es recomendable exponer dichas máquinas a la red de redes; obviamente si vais a trabajar con dicho sistema de

continuo veréis que muchos auditores lo tienen como sistema base pero si estáis en fases iniciales, esa es mi recomendación.

Respecto a los cambios de Kali Linux, en su nueva versión tiene un kernel 4.0 basado en Debian Jessie y obviamente han actualizado su arsenal de herramientas y se ha convertido en una distribución de liberación continua. Respecto al entorno de escritorio ahora tenemos a Gnome 3 -pero como dije anteriormente- yo me decanto por XFCE, así que mostraré como instalarlo.

Sin más que añadir, ya podríamos proceder a descargar la imagen del sistema, para eso nos dirigimos a: <https://www.kali.org/downloads/>

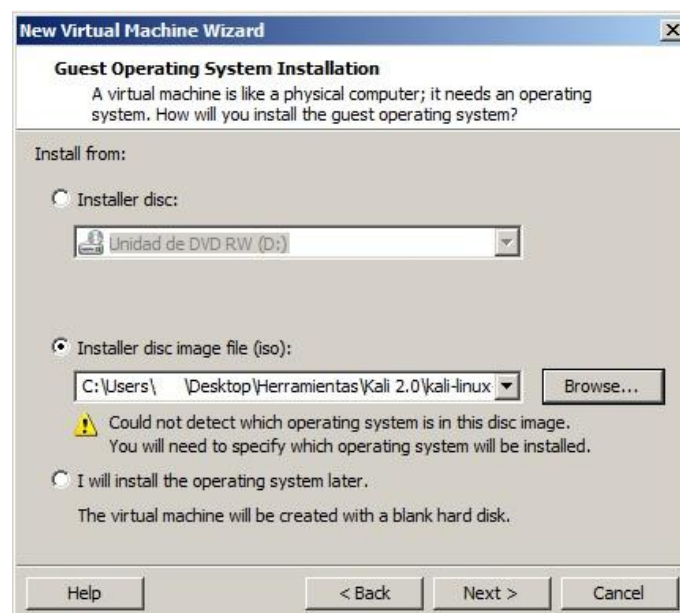
Una vez descargada les recomendaría comprobar que se trata de la imagen original así que procederemos a comprobar su hash SHA-1:

File	Checksum
<input checked="" type="checkbox"/> C:\Users\... \Desktop\Herramientas\Kali 2.0\kali-linux-2.0-amd64.iso	aaeb89a78f155377282f81a785aa1b38ee5f8ba0

Como podemos ver los hash coinciden, por consiguiente ya podemos comenzar con la creación de la máquina virtual y la instalación de Kali Linux.

## CREACIÓN DE LA MÁQUINA VIRTUAL: VMWARE

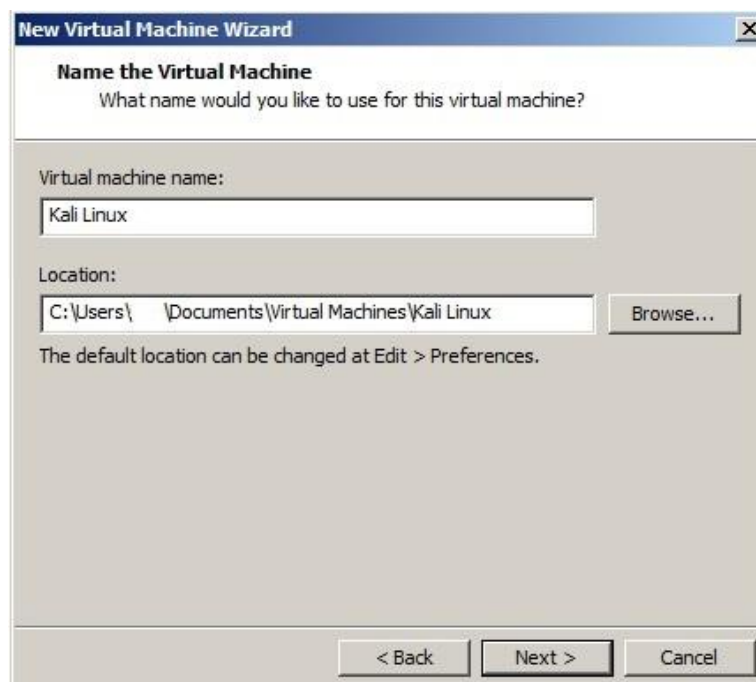
Comenzaremos abriendo VMware y creando una nueva máquina virtual, en esta ocasión seleccionaremos configuración típica y cargaremos la ISO de tal manera:



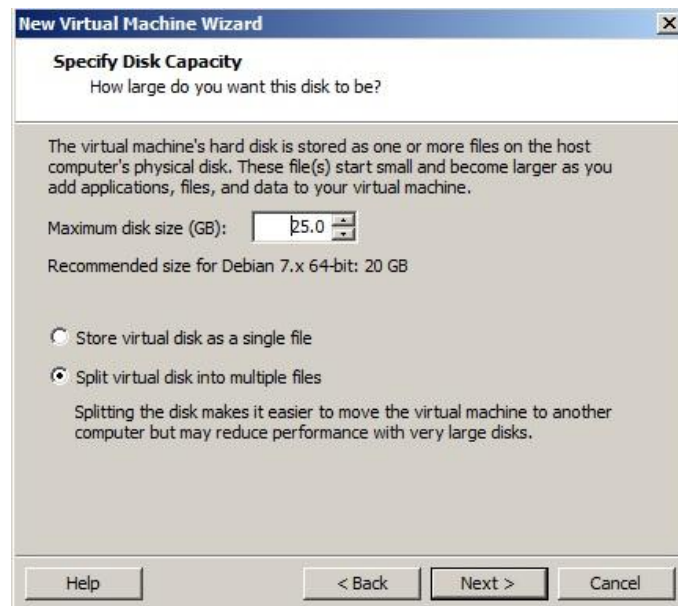
El paso siguiente, prosiguiendo con la instalación, es seleccionar Debian 7.x y la arquitectura que corresponda, en mi caso 64 bit (en caso de que tengan la opción Debian 8 seleccionarla, pues sería la correspondiente a Debian Jessie):












Continuamos seleccionando el nombre de la máquina, que en mi caso, será Kali Linux:



En la siguiente ventana nos pide especificar el tamaño del disco virtual, en mi caso pondré 25 GB y dejaré la segunda opción seleccionada del siguiente modo:



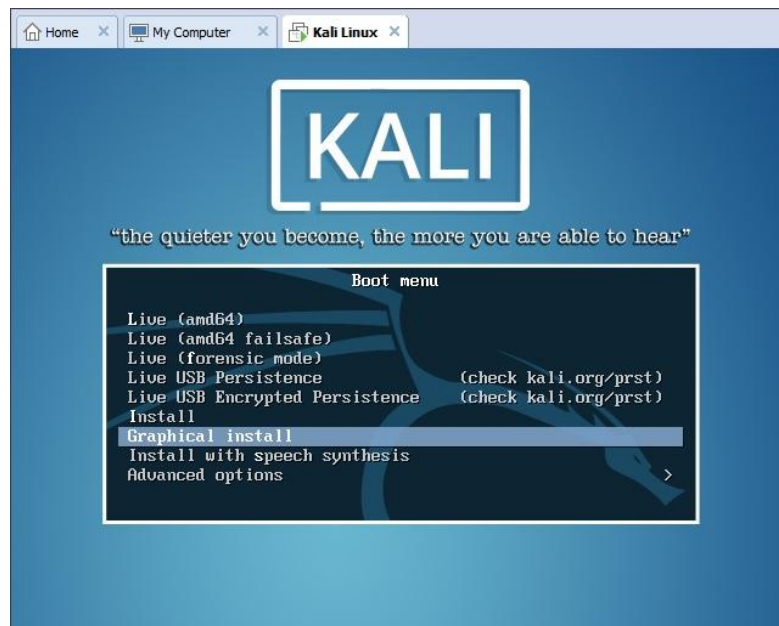
Luego solo nos quedaría finalizar el proceso de creación y ya tendríamos nuestra máquina virtual. Para finalizar vamos a configurar la red, en mi caso la pondré en modo adaptador puente y añadiré un poquito más de memoria de acceso aleatorio (RAM), el resultado final sería:

Device	Summary
 Memory	1.5 GB
 Processors	1
 Hard Disk (SCSI)	25 GB
 CD/DVD (IDE)	Using file C:\Users\
 Network Adapter	Bridged (Automatic)
 USB Controller	Present
 Sound Card	Auto detect
 Printer	Present
 Display	Auto detect

En este punto hemos finalizado la creación y configuración de nuestra máquina virtual. En el próximo apartado procederemos a instalar Kali Linux.

# INSTALACIÓN DE KALI LINUX

Una vez arrancada la máquina seleccionaremos la instalación gráfica:



Cuando accedemos al modo gráfico seleccionaremos nuestro teclado, ubicación e idioma (obviaré estos pasos pues únicamente es dar clicks). A continuación nos pedirá nuestro hostname, obviamente podéis poner el que queráis:

Configurar la red

Por favor, introduzca el nombre de la máquina.

El nombre de máquina es una sola palabra que identifica el sistema en la red. Consulte al administrador de red si no sabe qué nombre debería tener. Si está configurando una red doméstica puede inventarse este nombre.

Nombre de la máquina:

Luego nos pedirá un nombre de dominio el cual dejaremos en blanco, y tras eso tocará rellenar la clave de superusuario.

Configurar usuarios y contraseñas

Necesita definir una contraseña para el superusuario («root»), la cuenta de administración del sistema. Podría tener graves consecuencias que un usuario malicioso o un usuario sin la debida cualificación tuviera acceso a la cuenta del administrador del sistema, así que debe tener cuidado y elegir un la contraseña para el superusuario que no sea fácil de adivinar. No debería ser una palabra que se encuentre en el diccionario, o una palabra que pueda asociarse fácilmente con usted.

Una buena contraseña debe contener una mezcla de letras, números y signos de puntuación, y debe cambiarse regularmente.

La contraseña del usuario «root» (administrador) no debería estar en blanco. Si deja este valor en blanco, entonces se deshabilitará la cuenta de root creará una cuenta de usuario a la que se le darán permisos para convertirse en usuario administrador utilizando la orden «sudo».

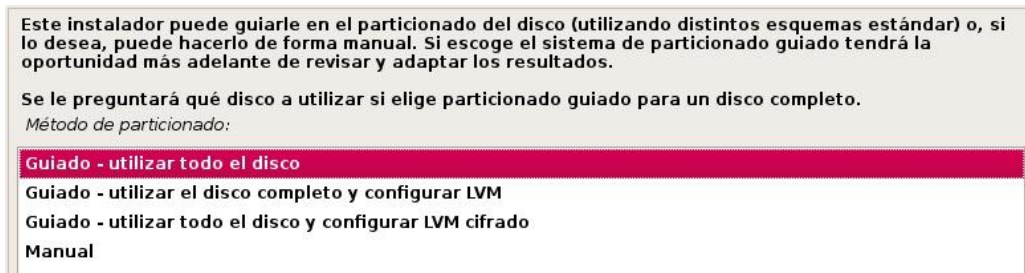
Tenga en cuenta que no podrá ver la contraseña mientras la introduce.

Clave del superusuario:

Por favor, introduzca la misma contraseña de superusuario de nuevo para verificar que la introdujo correctamente.

Vuelva a introducir la contraseña para su verificación:

Seguiremos configurando el reloj para que se ajuste a nuestra zona horaria y llegaremos a la zona de particionado de discos, como dije va ser una instalación desde la perspectiva de un novato, así que seleccionaremos guiado utilizando todo el disco:



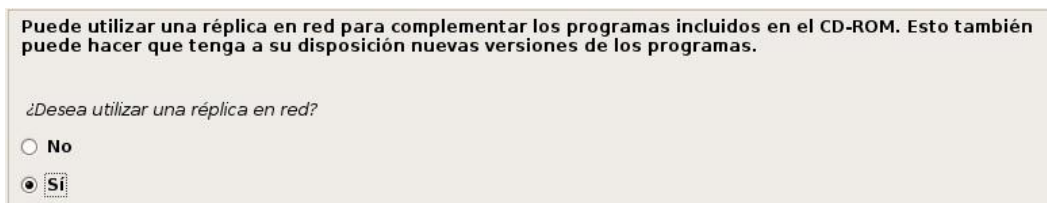
Seleccionaremos el único disco que tenemos y luego utilizaremos todos los ficheros en una partición:



Finalizamos el particionado y escribimos los cambios en el disco:



Luego nos quedaría confirmar la operación y comenzaría el proceso de instalación del sistema. A continuación nos pide si deseamos utilizar una réplica de red, lo dejaremos en sí pues es fundamental para la instalación desde los repositorios de Kali Linux:



El proxy es opcional, en mi caso lo dejaré en blanco. Ahora toca instalar el GRUB y lo vamos a instalar en el registro principal de arranque así que seleccionamos la opción por defecto:

Parece que esta instalación es el único sistema operativo en el ordenador. Si esto es así, puede instalar sin riesgos el cargador de arranque GRUB en el registro principal de arranque del primer disco duro.

**Aviso:** Si el instalador no pudo detectar otro sistema operativo instalado en el sistema, la modificación del registro principal de arranque hará que ese sistema operativo no puede arrancarse. Sin embargo, podrá configurar GRUB manualmente más adelante para arrancarlo.

¿Desea instalar el cargador de arranque GRUB en el registro principal de arranque?

No

Sí

En este paso seleccionaremos el dispositivo donde vamos a instalar el cargador de arranque:

Ahora debe configurar el sistema recién instalado para que sea arrancable, instalando para ello el cargador GRUB en un dispositivo del que se pueda arrancar. La forma habitual de hacerlo es instalar GRUB en el registro principal de arranque («master boot record») del primer disco duro. Si lo prefiere, puede instalar GRUB en cualquier otro punto del disco duro, en otro disco duro, o incluso en un disquete.

Dispositivo donde instalar el cargador de arranque:

Introducir el dispositivo manualmente

/dev/sda

Y tras seleccionarlo habremos finalizado la instalación de nuestro Kali Linux satisfactoriamente:

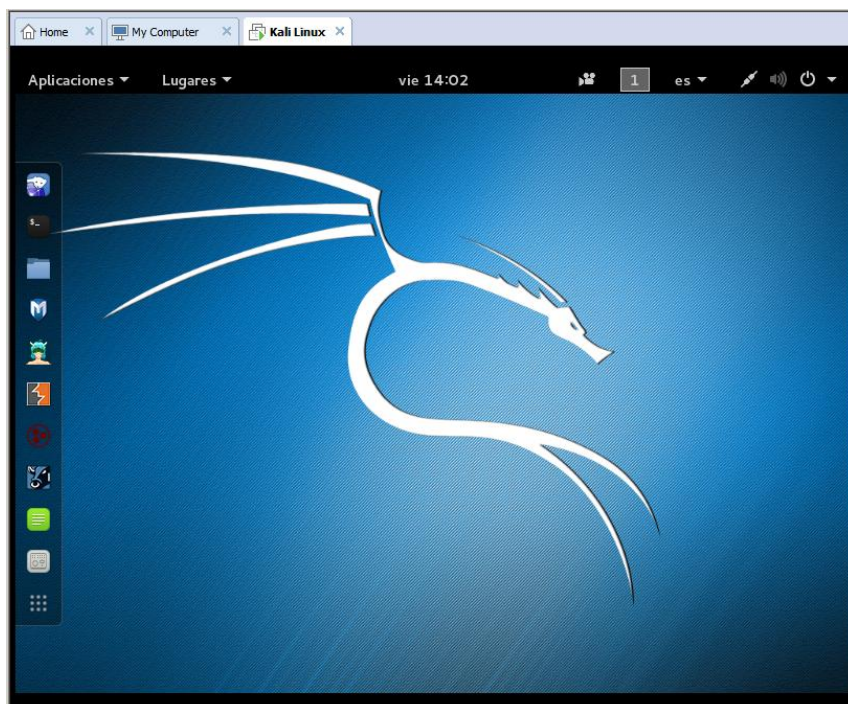
Terminar la instalación



Instalación completada

La instalación se ha completado. Ahora podrá arrancar el nuevo sistema. Asegúrese de extraer el disco de instalación (CD-ROM o disquetes) para que el sistema arranque del disco en lugar de reiniciar la instalación.

Tras reiniciar el sistema e ingresar nuestras credenciales (root) el resultado final será:





¡Perfecto! ahora ya tendremos nuestro Kali Linux listo para usarlo, pero obviamente nos queda el proceso de post-instalación que es casi tan importante o más que el proceso de instalación.

Lo primero será comprobar que nuestro sources.list contiene todos los repositorios de Kali (<http://docs.kali.org/general-use/kali-linux-sources-list-repositories>), para eso simplemente ejecutaremos:

```
cat /etc/apt/sources.list
```

Como podemos comprobar todo está correcto:

```
root@blackbox:~# cat /etc/apt/sources.list
#
# deb cdrom:[Debian GNU/Linux 2.0_Sana - Official Snapshot amd64 LIVE/INSTALL Binary 20150811-08:02]/ sana contrib main non-free
#deb cdrom:[Debian GNU/Linux 2.0_Sana - Official Snapshot amd64 LIVE/INSTALL Binary 20150811-08:02]/ sana contrib main non-free
deb http://http.kali.org/kali sana main non-free contrib
deb-src http://http.kali.org/kali sana main non-free contrib
deb http://security.kali.org/kali-security/ sana/updates main contrib non-free
deb-src http://security.kali.org/kali-security/ sana/updates main contrib non-free
root@blackbox:~#
```

Así que ahora toca actualizar nuestro Kali Linux y mantenerlo al día, de modo que ejecutaremos:

```
apt-get clean && apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y
```

La salida de mi terminal:

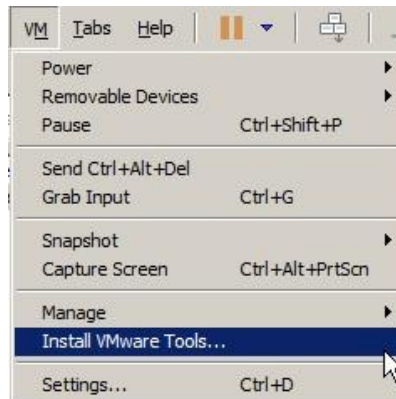
```
root@blackbox:~# apt-get clean && apt-get update && apt-get upgrade -y && apt-get dist-upgrade -y
Obj http://security.kali.org sana/updates InRelease
Obj http://http.kali.org sana InRelease
Obj http://http.kali.org sana/main Sources
Obj http://security.kali.org sana/updates/main Sources
Des:1 http://security.kali.org sana/updates/contrib Sources [20 B]
Obj http://http.kali.org sana/non-free Sources
Des:2 http://security.kali.org sana/updates/non-free Sources [20 B]
Des:3 http://http.kali.org sana/contrib Sources [58,3 kB]
Obj http://http.kali.org sana/main amd64 Packages
Obj http://security.kali.org sana/updates/main amd64 Packages
Obj http://security.kali.org sana/updates/contrib amd64 Packages
Obj http://http.kali.org sana/non-free amd64 Packages
Obj http://security.kali.org sana/updates/non-free amd64 Packages
Obj http://http.kali.org sana/contrib amd64 Packages
Ign http://http.kali.org sana/contrib Translation-es_ES
```

Después de esto, podemos proceder a instalar los respectivos headers de Linux:

```
aptitude install build-essential Linux-headers-$(uname -r)
```

```
root@blackbox:~# aptitude install build-essential linux-headers-$(uname -r)
Se instalarán los siguiente paquetes NUEVOS: have the following installed...
  linux-compiler-gcc-4.9-x86{a} linux-headers-4.0.0-kali1-amd64
  linux-headers-4.0.0-kali1-common{a} linux-kbuild-4.0{a}
0 paquetes actualizados, 4 nuevos instalados, 0 para eliminar y 0 sin actualizar.
Necesito descargar 5.652 kB de ficheros. Después de desempaquetar se usarán 36,0 MB.
¿Quiere continuar? [Y/n/?] Y
Des: 1 http://http.kali.org/kali/ sana/main linux-compiler-gcc-4.9-x86 amd64 4.0.4-1+kali2 [301 kB] gcc...
Des: 2 http://http.kali.org/kali/ sana/main linux-kbuild-4.0 amd64 4.0.2-1kali1 [175 kB]
[the path "/usr/bin/gcc" appears to be a valid path to the gcc binary.
Des: 3 http://http.kali.org/kali/ sana/main linux-headers-4.0.0-kali1-common amd64 4.0.4-1+kali2 [4.710 kB]
9% [2 linux-kbuild-4.0 97,7 kB/175 kB 56%] [3 linux-headers-4.0.0-kali1-common 115 kB/4
[the path "" is not a valid path to the 4.0.0-kali1-amd64 kernel headers.
```

Terminada la instalación de los headers, podemos proceder a introducir las tools de VMware para ajustar libremente la resolución de nuestro sistema:



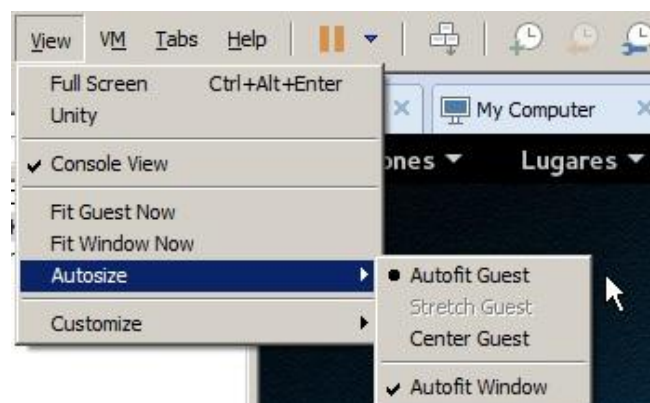
Tras introducir las tools de VMware, procedemos a extraer el archivo, acceder al directorio e instalarlas:

```
root@blackbox:~# cd Escritorio/
root@blackbox:~/Escritorio# ls
VMwareTools-9.9.2-2496486.tar.gz
root@blackbox:~/Escritorio# tar -xf VMwareTools-9.9.2-2496486.tar.gz
root@blackbox:~/Escritorio# ls
VMwareTools-9.9.2-2496486.tar.gz  vmware-tools-distrib
root@blackbox:~/Escritorio# cd vmware-tools-distrib/
root@blackbox:~/Escritorio/vmware-tools-distrib# ls
bin  doc  etc  FILES  INSTALL  installer  lib  vmware-install.pl
root@blackbox:~/Escritorio/vmware-tools-distrib# perl vmware-install.pl
Creating a new VMware Tools installer database using the tar4 format.

Installing VMware Tools.

In which directory do you want to install the binary files?
[/usr/bin] █
```

Una vez finalizada la instalación de dichas herramientas, estaremos listos para ajustar la forma:



Hasta aquí llegaría la parte de la post-instalación básica.

## INSTALACIÓN DE XFCE

Vamos a proceder a instalar otro entorno de escritorio, en esta ocasión y como dije anteriormente, instalaremos XFCE y para ello escribimos en nuestra terminal:

```
apt-get install kali-defaults kali-root-login desktop-base xfce4 xfce4-places-plugin  
xfce4-goodies
```

```
root@blackbox:~# apt-get install kali-defaults kali-root-login desktop-base xfce4  
4 xfce4-places-plugin xfce4-goodies  
Leyendo lista de paquetes... Hecho  
Creando árbol de dependencias  
Leyendo la información de estado... Hecho  
desktop-base ya está en su versión más reciente.  
kali-defaults ya está en su versión más reciente.  
kali-root-login ya está en su versión más reciente.  
Se instalarán los siguientes paquetes extras:  
  alsabase exo-utils gstreamer0.10-alsa gtk2-engines-xfce hddtemp libburn4  
  libexo-1-0 libexo-common libexo-helpers libgarcon-1-0 libgarcon-common
```

Ahora instalaremos lightdm mediante la siguiente sintaxis:

```
apt-get install lightdm xfce4
```

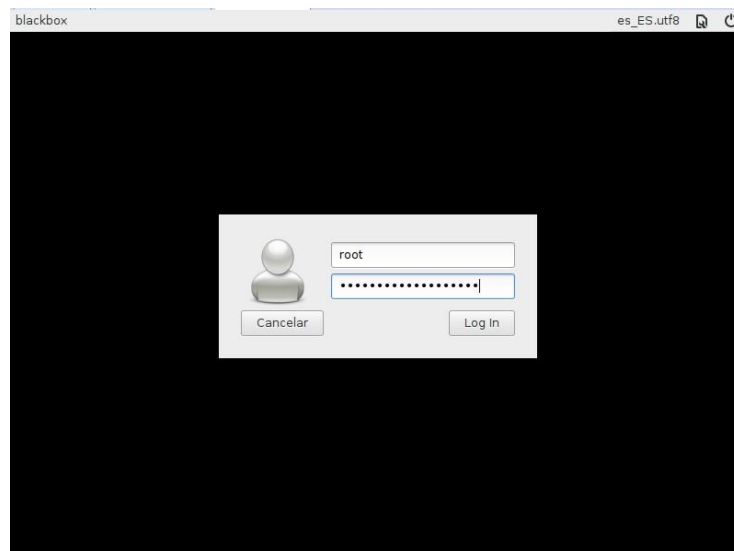
Y configuraremos la sesión desde:

```
/usr/share/xsessions/
```

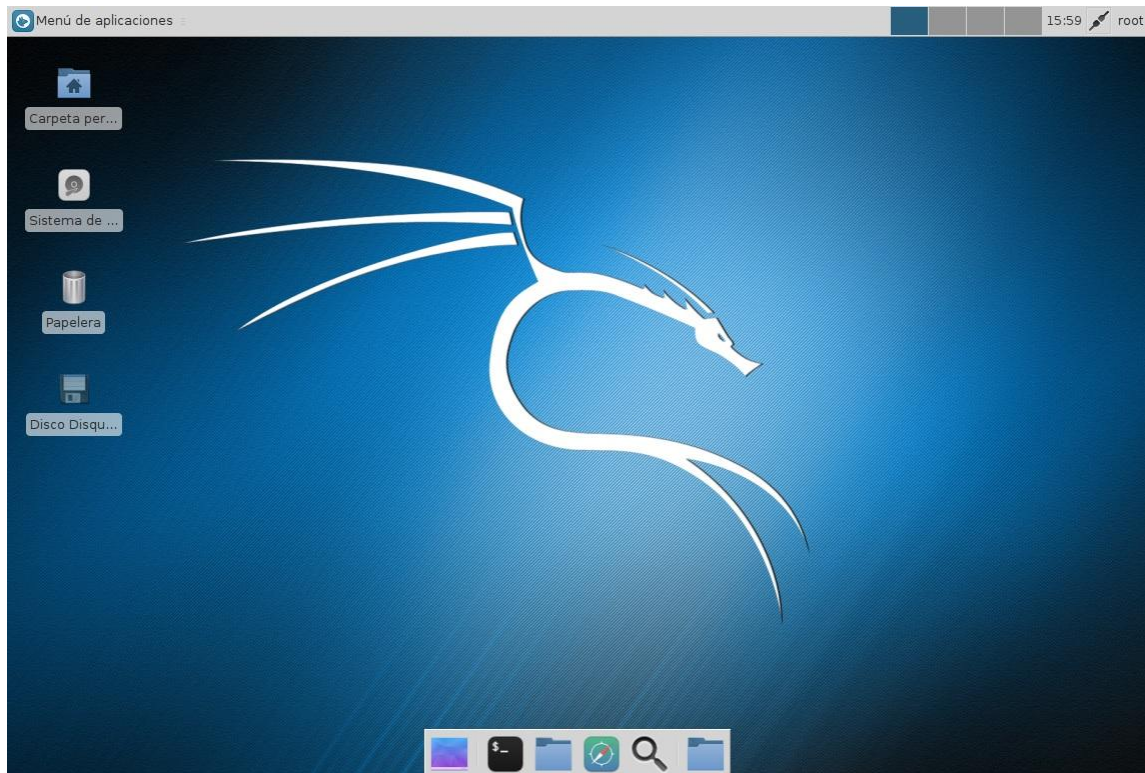
Utilizaremos nuestro editor favorito en mi caso nano:

```
GNU nano 2.2.6          Fichero: lightdm-xsession.desktop  
[Desktop Entry]  
Version=1.0  
Name=Default Xsession  
Exec=startxfce4  
Icon=  
Type=Application
```

Tras editar el gestor de sesiones debería arrancar nuestro xfce, si reiniciamos veremos que los cambios se han efectuado correctamente:



El resultado final:



Yo lo dejaría aquí pues no me gusta sobre cargar el sistema de efectos innecesarios o personalizarlo, pero como reconozco que visualmente no queda muy atractivo vamos a personalizar un poco el sistema. Para personalizar nuestro xfce nos podemos dirigir a: <http://xfce-look.org> , donde encontraremos diversas variedades de wallpapers, iconos, temas, etc...

Obviaré que saben instalar temas e iconos pues simplemente es moverlos a la ruta **/usr/share/themes** o **/usr/share/icons** (dependiendo de lo que estén instalando).

Luego en el menú de aplicaciones nos dirigimos a configuración y en apariencia seleccionaremos los temas e iconos instalados.

Y luego de este proceso de personalización, podría quedaros algo similar a la siguiente imagen:



Con esto doy por concluida la entrega, ha sido un placer guiaros por este proceso.