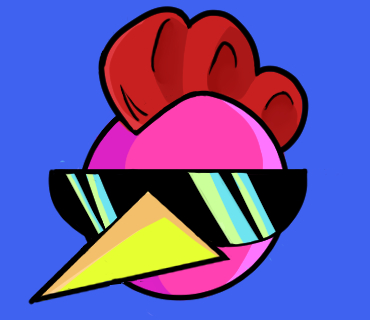
Manual Técnico del Software



Dispositivo de Seguridad informática, para el cumplimiento de la ley 25.326 sobre la protección de datos personales

Autores:

Vaz Nicolas

Blanco Inti

Octubre del 2021

Índice:

|  |
| --- |
| Introducción |
| Componentes del sistema |
| Requerimientos del sistema |
| Inicio de Sesión |
| Configuraciones:   * Acceder a una red WiFi * Cambiar la resolución de la pantalla * Búsqueda y descarga de actualizaciones * Ser Usuario ROOT * Instalacion de PuTTY * Instalacion de UltraVNC |
| ¿Desea Conocer más de SecurityKit? |

INTRODUCCION

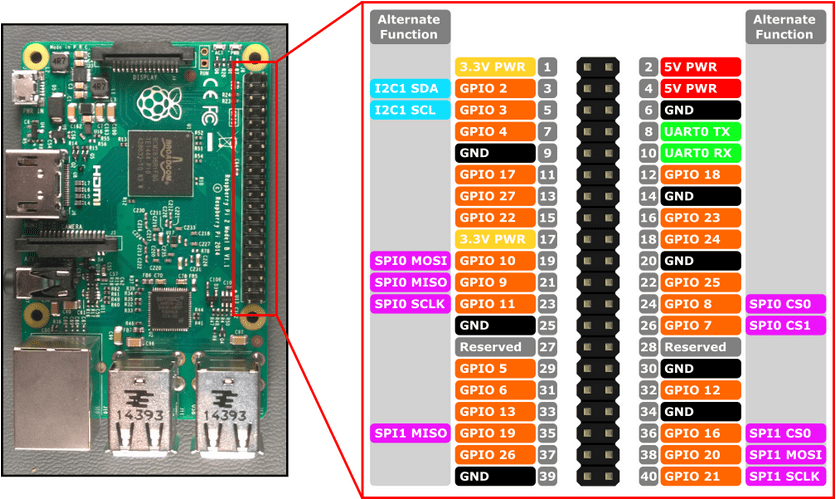
Este proyecto a sido concebido debido a la necesidad de proteger la identidad y los datos de los usuarios debido a los riesgos que abundan a través de las redes que usamos dia a dia

Queremos cumplir la ley 25.326, que tiene por objetivo la protección integral de los datos personales asentados en archivos, registros, bancos de datos, u otros medios técnicos de tratamiento de datos, sean éstos públicos, o privados destinados a dar informes, para garantizar el derecho al honor y a la intimidad de las personas, así como también el acceso a la información que sobre las mismas se registre.

Para eso, diseñamos este dispositivo de Ciberseguridad, que mantendrá segura su red, y alejada de invasores ajenos con intenciones maliciosas

COMPONENTES DEL SISTEMA

**Raspberry Pi 3B:**



Incorpora una CPU Cortex-A53 de cuatro núcleos, 64bit y 1.2Ghz, el cual mejora su velocidad de respuesta en un 50% en comparación a su versión anterior (RPi v2 modelo B) y diez veces más rápida que la primera Raspberry Pi.

La Raspberry Pi 3 es compatible con todos los accesorios para la Raspberry Pi B+ y V2 modelo B, ya que mantiene el mismo conector GPIO para la conexión sensores, periféricos y otros.

También incluye conexión Wi-Fi de 802.11n y Bluetooth 4.1, con lo cual ya no dependerás de una conexión tipo Ethernet para acceder a Internet o gracias a la conexión Bluetooth conectar un teclado o mouse inalámbrico para controlar tu Raspberry Pi 3, así como también comunicarte de manera inalámbrica con sensores y otros dispositivos.

Características:

* Chipset Broadcom BCM2837 a 1,2 GHz
* ARM Cortex-A53 de 64 bits y cuatro núcleos
* LAN inalámbrica 802.11 b/g/n
* Bluetooth 4.1 (posee modo bajo consumo)
* Coprocesador multimedia de doble núcleo Videocore IV®
* Memoria LPDDR2 de 1 GB
* Compatible con todas las últimas distribuciones de ARM GNU/Linux y Windows 10 IoT
* 1x Puerto Ethernet 10/100
* 1x Conector de vídeo/audio HDMI
* 1x Conector 3.5mm audio/video compuesto.
* 4x Puertos USB 2.0
* 40x Pines GPIO
* Antena de chip (WiFi y Bluetooth integrados)
* Conector de pantalla DSI
* Ranura de tarjeta microSD
* Dimensiones: 85 x 56 x 17 mm

**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.

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 DVD o utilizar una distribución Live desde USB. También permite la instalación vía red y brinda imágenes para la descarga de máquinas virtuales prefabricadas con las herramientas instaladas de VMWare.

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

Características:

* Permite compilar kernels para arquitecturas RISC desde distribuciones para amd64 e i386.
* Permite la personalización del paquete source mediante Debian Tools.
* Admite la recompilación del núcleo lo que permite agregar drivers, parches o nuevas funcionalidades que no estén incluidas en el kernel original.

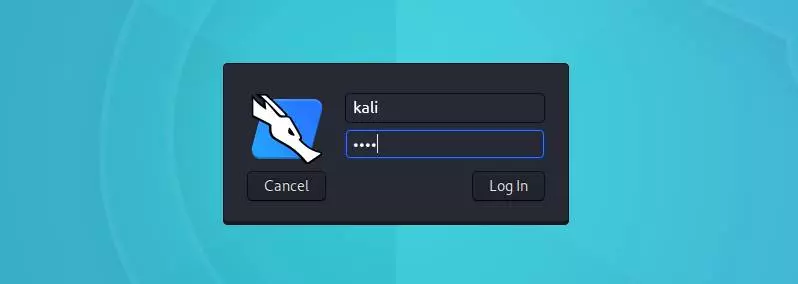
REQUERIMIENTOS DEL SISTEMA

Para lograr utilizar nuestro sistema de seguridad informática, se debe cumplir ciertos requerimientos de hardware y conocimiento del usuario:

1. Se debe poseer una conexión a una red, ya que el sistema fue creado para la protección de datos de los usuarios que usan comúnmente redes alámbricas o inalámbricas.
2. Se recomienda tener un teclado y una pantalla para realizar las configuraciones iniciales a la Raspberry Pi.
3. Se recomienda tener conocimientos de seguridad informática, para sacar el máximo potencial al sistema.

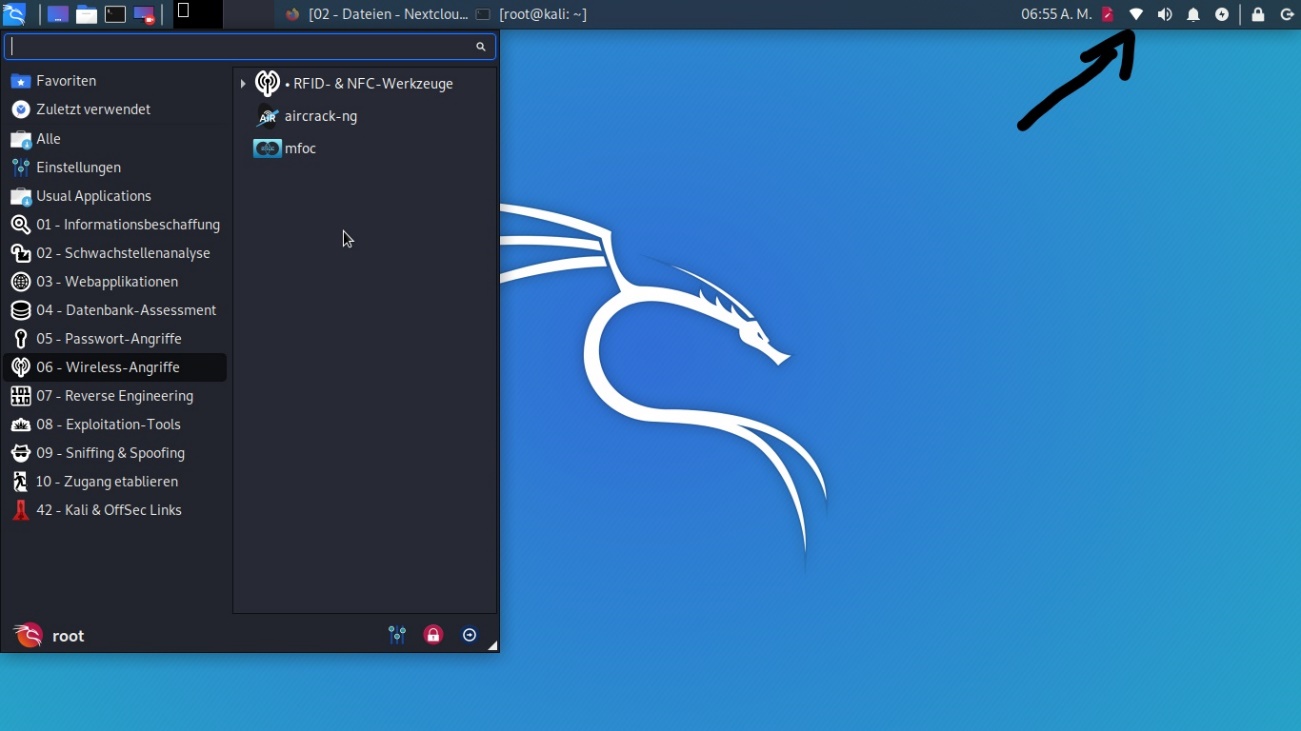
INICIO DE SESION

Si es la primera vez iniciando sesión en tu dispositivo Kali Linux, la contraseña y el usuario son kali



ACCEDER A UNA RED WIFI

Para acceder a una red WiFi, clickee sobre el icono señalado en pantalla, y busque su red



Por ultimo, ingrese su contraseña de su red wifi, y ya estará en linea

CAMBIAR LA RESOLUCION DE NUESTRA PANTALLA

Para cambiar la resolución de nuestra pantalla, de nuestra Raspberry Pi, tendremos que editar el archivo config.txt y desactivar el driver GL en nuestra Raspberry Pi.

Una vez sabemos lo que tenemos que hacer, configurar la pantalla de nuestra Raspberry Pi será cuestión de dos minutos. Lo haremos de la siguiente manera:

1. Abrimos un terminal y escribimos lo siguiente:

**sudo raspi-config**

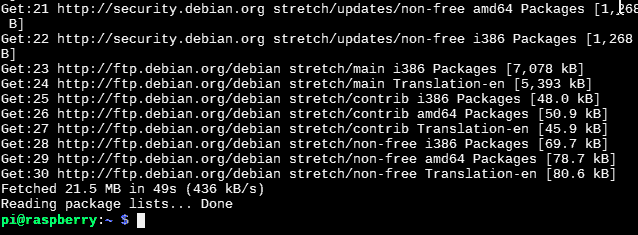
1. Vamos al apartado Advanced options y luego a GL driver.
2. Elegimos «Legacy». Esto puede que no sea necesario. Lo siguiente, sí.
3. Editamos el archivo config.txt que está en la carpeta /boot de nuestra tarjeta micro SD. Esto podemos hacerlo de diferentes maneras: desde un editor de texto cualquiera en Linux, macOS o Windows o desde el sistema operativo de la Raspberry Pi. Si elegimos esta última opción, tenemos que abrir un terminal y escribir sudo nano /boot/config.txt, hacemos las modificaciones, guardamos y salimos.
4. Con el archivo abierto, lo que tenemos que modificar son las líneas en donde pone «overscan». Tenemos que quitar la almohadilla para activar la linea (cambia el color a blanco) y probar valores hasta que la pantalla encaje. Usaremos números positivos si vemos barras negras y números negativos si la imagen sobresale. No veremos nada hasta reiniciar el equipo.
5. Reiniciamos.

BUSQUEDA Y DESCARGA DE ACTUALIZACIONES

Una de las operaciones para las que usaremos APT con más frecuencia es realizar la actualización de los paquetes que tenemos instalados. Actualizar nuestro software es importante tanto para obtener nuevas funciones, como para solventar posibles errores de seguridad.

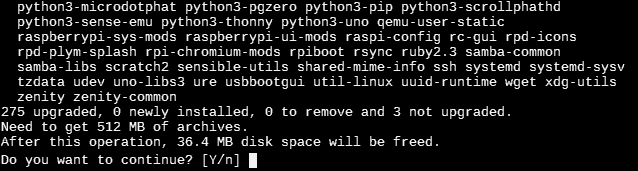
En APT el proceso de actualización se realiza en dos pasos. Por un lado, el comando 'update' actualiza el cache de paquetes local. Busca nuevos cambios, comparando con la información contenida en los repositorios, pero no descarga ni instala ningún paquete.

**sudo apt-get update**



Para realizar realmente la instalación de los paquetes actualizados, que previamente hemos determinado cuales son con el comando 'update', empleamos el comando 'upgrade'.

**sudo apt-get upgrade**



**Uso permanente vs temporal**

Hay algunos casos en los que es posible que deba utilizar superusuario, root, durante un período de tiempo prolongado. En estos casos, podemos acceder fácilmente a la cuenta de root con un simple **sudo su** (que pedirá la contraseña del usuario actual), seleccionando el icono de la terminal raíz en el menú Kali, o alternativamente usando **su -** (que pedirá la contraseña del usuario root), si ha establecido una contraseña para la cuenta raíz que conoce. Cuando termine, **exit** o CTRL + D nos sacará de este caparazón elevado.

Sin embargo, puede haber otras ocasiones en las que desee utilizar la raíz en varias sesiones sin la molestia de aumentar los privilegios. En estas situaciones, necesitaremos instalar un paquete y hacer algunas modificaciones para habilitar completamente la cuenta de root para su uso debido a razones de seguridad de mantener la cuenta de root deshabilitada de forma predeterminada.

**Habilitando la cuenta root**

Lo primero que debe hacer es establecer una contraseña de root, que debería ser diferente a la contraseña del usuario actual (en este caso, **kali**). Podemos hacer esto haciendo lo siguiente:

kali @ kali: ~ $ sudo passwd

[sudo] contraseña para kali:

Nueva contraseña:

Reescriba nueva contraseña:

passwd: contraseña actualizada correctamente

kali @ kali: ~ $

**Habilitación de root para SSH**

Si miramos **/ etc / ssh / sshd\_config** veremos una línea **PermitRootLogin**. Querremos cambiar esta línea para que coincida con nuestro caso de uso.

kali@kali:~$ grep PermitRootLogin /etc/ssh/sshd\_config

#PermitRootLogin prohibit-password

# the setting of "PermitRootLogin without-password".

kali@kali:~$

kali@kali:~$ man sshd\_config | grep -C 1 prohibit-password

PermitRootLogin

Specifies whether root can log in using ssh(1). The argument must be yes, prohibit-password, forced-commands-only, or no. The default

is prohibit-password.

If this option is set to prohibit-password (or its deprecated alias, without-password), password and keyboard-interactive authentication

are disabled for root.

kali@kali:~$

kali@kali:~$ sudo systemctl restart ssh

kali@kali:~$

Si hemos configurado el inicio de sesión basado en la clave SSH para la cuenta raíz, simplemente podemos descomentar la línea correspondiente y continuar. De lo contrario, deberíamos cambiar PermitRootLogin para que sea yes, lo que nos permitirá ingresar una contraseña.

Habilitación de root para el inicio de sesión de GNOME y KDE

Primero instalaremos **kali-root-login** para cambiar varios archivos de configuración que nos permitirán iniciar sesión en la cuenta raíz a través de GNOME GDM3 y el indicador de inicio de sesión de KDE. Este paso no es necesario cuando se utilizan otros entornos de escritorio.

kali@kali:~$ sudo apt -y install kali-root-login

Reading package lists... Done

Building dependency tree

Reading state information... Done

The following NEW packages will be installed:

kali-root-login

0 upgraded, 1 newly installed, 0 to remove and 1516 not upgraded.

Need to get 6,776 B of archives.

After this operation, 33.8 kB of additional disk space will be used.

Get:1 http://kali.download/kali kali-rolling/main amd64 kali-root-login all 2019.4.0 [6,776 B]

Fetched 6,776 B in 1s (10.9 kB/s)

Selecting previously unselected package kali-root-login.

(Reading database ... 333464 files and directories currently installed.)

Preparing to unpack .../kali-root-login\_2019.4.0\_all.deb ...

Adding 'diversion of /etc/gdm3/daemon.conf to /etc/gdm3/daemon.conf.original by kali-root-login'

Adding 'diversion of /etc/pam.d/gdm-password to /etc/pam.d/gdm-password.original by kali-root-login'

Adding 'diversion of /etc/pam.d/gdm-autologin to /etc/pam.d/gdm-autologin.original by kali-root-login'

Adding 'diversion of /etc/pam.d/lightdm-autologin to /etc/pam.d/lightdm-autologin.original by kali-root-login'

Adding 'diversion of /etc/pam.d/sddm to /etc/pam.d/sddm.original by kali-root-login'

Adding 'diversion of /etc/sddm.conf to /etc/sddm.conf.original by kali-root-login'

Unpacking kali-root-login (2019.4.0) ...

Setting up kali-root-login (2019.4.0) ...

Installing /usr/share/kali-root-login/daemon.conf as /etc/gdm3/daemon.conf

Installing /usr/share/kali-root-login/gdm-password as /etc/pam.d/gdm-password

Installing /usr/share/kali-root-login/gdm-autologin as /etc/pam.d/gdm-autologin

Installing /usr/share/kali-root-login/lightdm-autologin as /etc/pam.d/lightdm-autologin

Installing /usr/share/kali-root-login/sddm as /etc/pam.d/sddm

Installing /usr/share/kali-root-login/sddm.conf as /etc/sddm.conf

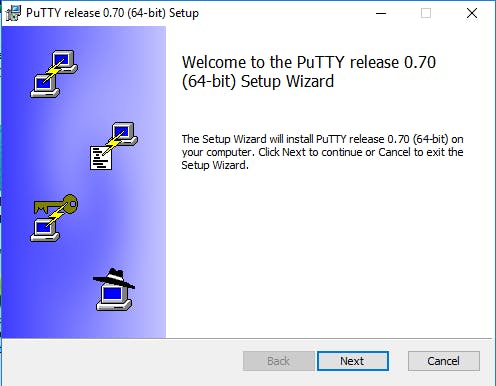
kali@kali:~$

Ahora podemos cerrar la sesión de nuestra cuenta de usuario no root e iniciar sesión en root con la contraseña que establecimos anteriormente.

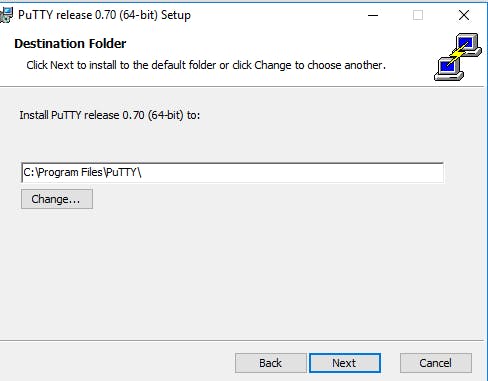
DESCARGA E INSTALACION DE PUTTY

Primero, descargaremos la versión más reciente de PuTTY haciendo click [aquí](https://www.chiark.greenend.org.uk/~sgtatham/putty/latest.html), recuerde que tiene que ser compatible según su arquitectura (si es de 32 o 64 bits)

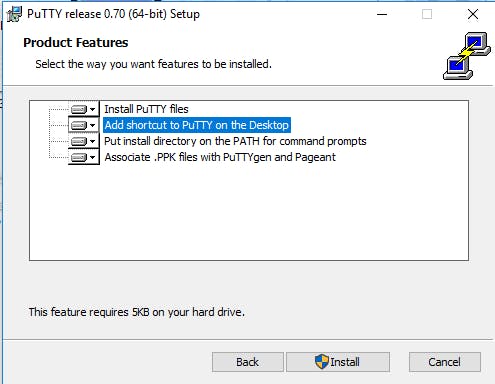
Despues de descargar PuTTY, este será el primer cuadro de dialogo que verá



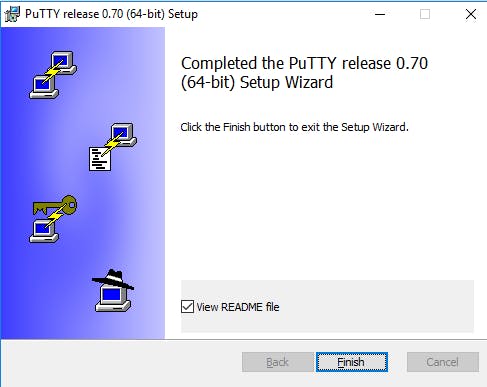
Cliquee en Next, y elija la carpeta donde se va a instalar el programa



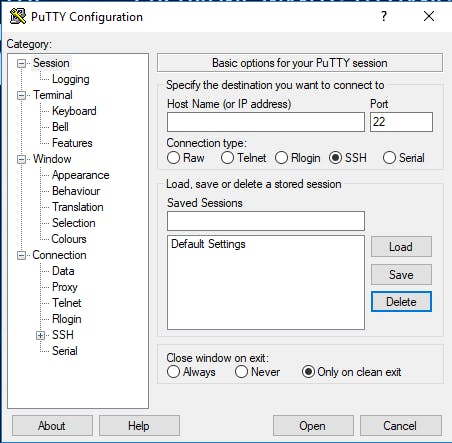
Asegúrese de que no haya ninguna marca roja en ninguno de los cuadros que se muestran a continuación y luego presione instalar



Cliquea en Finish



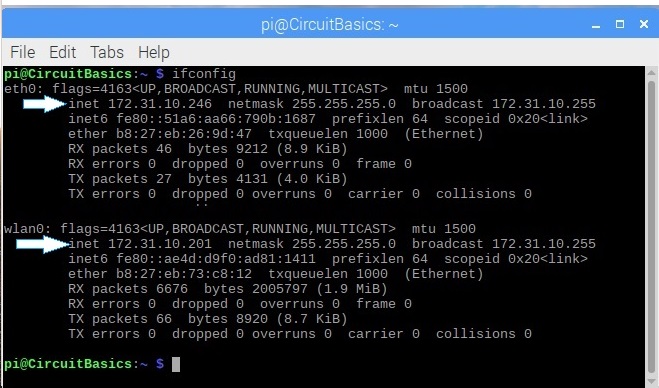
Ahora, este es el cuadro de dialogo que verá a la hora de iniciar la aplicación



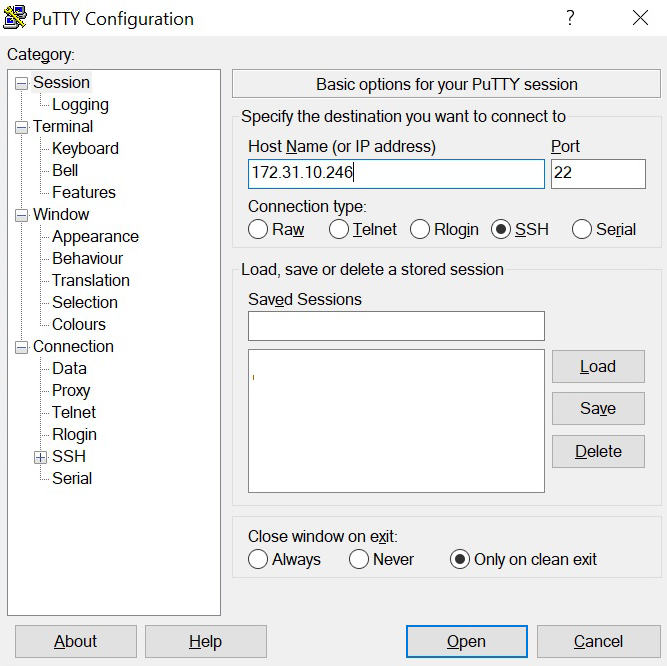
Ahora volvamos a nuestra Raspberry Pi.

Para conectarse mediante una conexión de red, abra su Raspberry Pi para determinar la dirección IP. La forma más sencilla de hacer esto es abrir el indicador de Terminal en el escritorio e ingresar ifconfig como se muestra a continuación. Si ha establecido una conexión WiFi, busque wlan0 y observe la entrada inet. En este caso, es 172.312.10.201.

Si está utilizando una conexión Ethernet, busque eth0 y observe la entrada inet (172.31.10.246 en este caso). Dependiendo de su configuración, puede tener dos direcciones, pero solo necesita seleccionar una. Tome nota de la dirección IP porque la necesitará para conectarse al Pi con PuTTY.



Esta vez, abra PuTTY e ingrese su dirección IP donde dice "Nombre de host (o dirección IP)".



Luego haga clic en "Abrir" para abrir la ventana de la terminal:



Por ultimo ingresa tu usuario y contraseña de la Raspberry Pi, y listo, ya puede usarla de forma remota.

DESCARGA E INSTALACION DE REALVNC

**Paso 1** Actualice el Kali Pi

Primero, carguemos Kali en nuestra Raspberry Pi. Conéctese a él a través de SSH o accediendo directamente. Siempre queremos ejecutar el comando apt-get update en una ventana de terminal para asegurarnos de que todas nuestras dependencias estén actualizadas y funcionando correctamente. Asegúrese de que el Pi y el dispositivo que está utilizando para conectarse al Pi estén en la misma red de área local inalámbrica o cableada.

**Paso 2**: instale el software del servidor VNC en el Kali Pi

Hay varias versiones de VNC, todas con diferentes propósitos, pero en este tutorial usaremos TightVNC, ya que está bien soportado, tiene mucha documentación en la comunidad Raspberry Pi y es fácil de instalar en cualquier versión de Pi.

Abra una ventana de comando en su Raspberry Pi y **escriba apt-get install tightvncserver**. Esto descargará e instalará el software. Cuando esté completo, escriba **tightvncserver**. Esto habilita el servicio TightVNC y requerirá que cree una contraseña para acceder a su dispositivo desde otra computadora. Continúe y cree uno ahora. Debe tener en cuenta que TightVNC solo puede configurar una contraseña de 8 caracteres al seleccionar una.

Una vez que ingrese una contraseña, le preguntará "¿Le gustaría ingresar una contraseña de solo lectura (y / n)?" Presione N, porque una contraseña de solo lectura solo le permitirá ver lo que se muestra en la máquina, pero no podrá controlarlo.

**Paso 3:** configure el servidor TightVNC en Kali Pi

Ahora, para poder acceder a nuestro Kali Pi de forma remota, necesitamos ejecutar TightVNC en él en el arranque. En nuestro Kali P, navegaremos hasta el directorio escribiendo cd /etc/init.d. A continuación, queremos crear un script de inicio, para que pueda usar el editor de texto que prefiera, pero a mí me gusta Vim. Si usa Vim, escriba vim /etc/init.d/vncboot para crear el script de inicio. A continuación, queremos insertar el siguiente script en el documento en blanco.

#!/bin/sh

### BEGIN INIT INFO

# Provides: vncboot

# Required-Start: $remote\_fs $syslog

# Required-Stop: $remote\_fs $syslog

# Default-Start: 2 3 4 5

# Default-Stop: 0 1 6

# Short-Description: Start VNC Server at boot time

# Description: Start VNC Server at boot time.

### END INIT INFO

USER=root

HOME=/root

export USER HOME

case "$1" in

start)

echo "Starting VNC Server"

#Insert your favoured settings for a VNC session

/usr/bin/vncserver :0 -geometry 1280x800 -depth 16 -pixelformat rgb565

;;

stop)

echo "Stopping VNC Server"

/usr/bin/vncserver -kill :0

;;

\*)

echo "Usage: /etc/init.d/vncboot {start|stop}"

exit 1

;;

esac

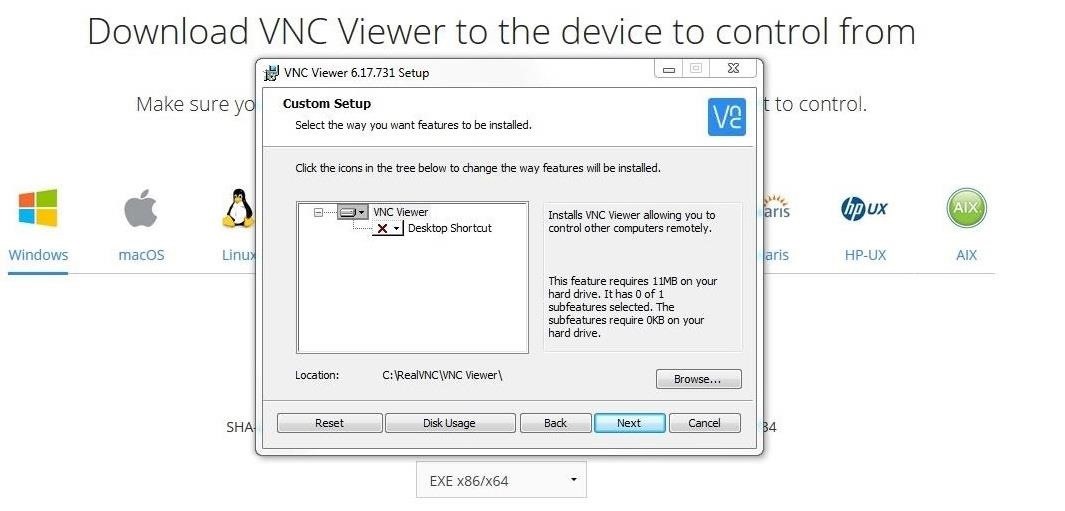
exit 0

Después de que todo ese texto esté en su lugar, guardaremos y saldremos presionando la tecla Esc y escribiendo: wq !. Una vez cerrado el documento, queremos agregar permisos a este nuevo script de inicio escribiendo **chmod 755 /etc/init.d/vncboot**. Cuando termine, queremos agregar las dependencias escribiendo **update-rc.d vncboot defaults**.

Reinicie el Kali Pi y el módulo VNC se agregará a la secuencia de inicio de inicio.

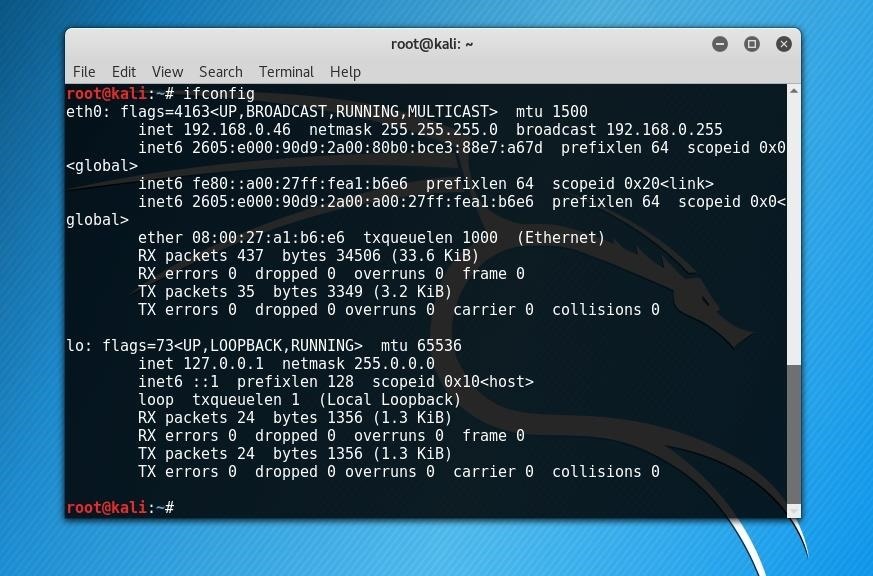
**Paso 4** Descargue e instale el cliente VNC

Ahora podemos usar cualquier cliente VNC que queramos, pero vamos a usar el "VNC Viewer" de RealVNC porque funciona en Linux, Android, y es uno de los pocos que también funciona en Windows e iOS. Puede descargar la versión que desee del sitio web de RealVNC. Una vez descargado, instálelo como lo haría con cualquier otro programa. En esta guía, usaré Windows.



**Paso 5** Encuentre la dirección IP de Kali Pi

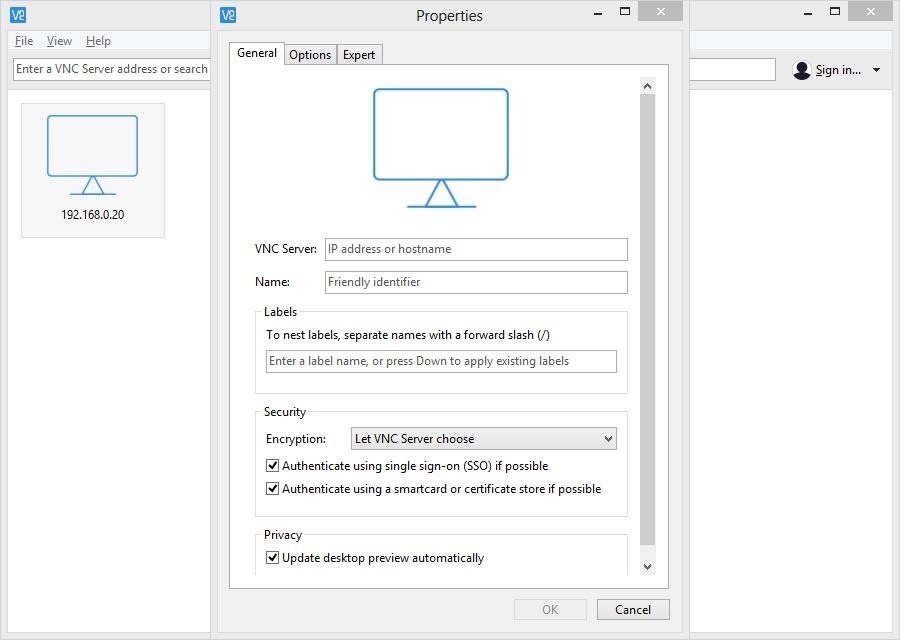
Después de instalar el software del cliente, queremos volver a nuestro Kali Pi sin cabeza. Nuevamente, conéctese ya sea mediante SSH o accediendo a él directamente, luego abra una terminal y escriba ifconfig. Anote la dirección IP local de Kali Pi; debería verse como "192.168.0.x".



**Paso 6** Conéctese al Kali Pi a través de nuestra computadora

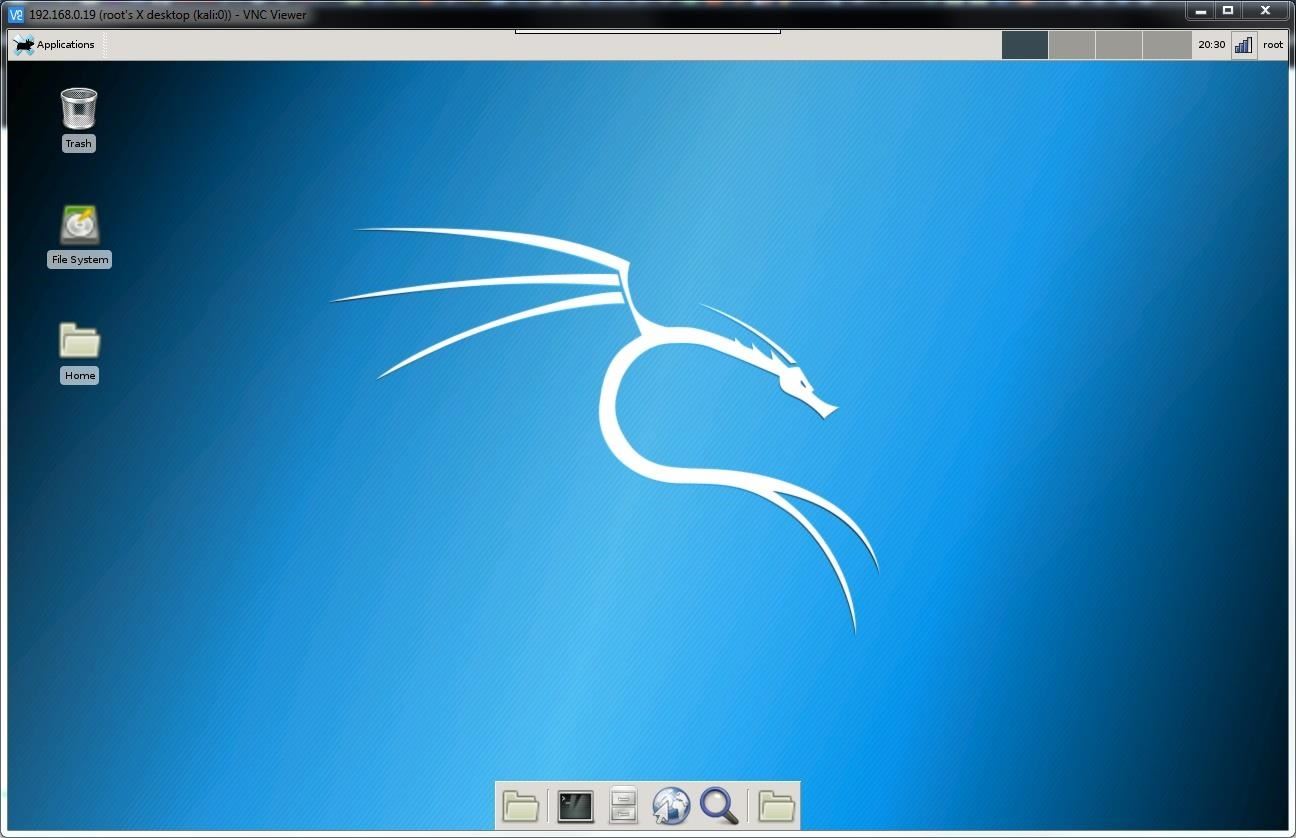
A continuación, regresemos a nuestra máquina con Windows y abramos la aplicación VNC Viewer. Las siguientes instrucciones pueden ser diferentes si lo está utilizando en otro sistema operativo.

En VNC Viewer, haga clic en la opción "Archivo" y luego en la pestaña "Nueva conexión". Ahora, agreguemos la dirección IP de Kali Pi al campo VNC Server. Puede guardarlo como cualquier nombre que le ayude a recordar este dispositivo en el campo Nombre. Presione "OK" para terminar y guardar la configuración.



Haga doble clic en su nueva conexión y, si tiene éxito, aparecerá una ventana que dice "La conexión a este servidor VNC no se cifrará". Debido a esto, no se recomienda usar esto fuera de su red si espera privacidad. Simplemente presione el botón "Continuar". Aparecerá otra ventana pidiendo la contraseña que creamos en el segundo paso.

Finalmente, ¡bam! Si la conexión fue exitosa, debería ver una pantalla como la que se muestra a continuación.



¿DESEA CONOCE MAS DE SECURITY KIT?

Contactenos a traves de nuestro [Instagram](https://www.instagram.com/security_kit/)

