Setting up Kali Linux on a Raspberry Pi 4

# Introduction

This guide is written for installing Kali Linux on a Raspberry Pi 4 (RP4). In this, I will assume you have some basic knowledge of the Linux command line as well as a Windows computer (which is what I will be using). This guide is being written with information taken from both NullByte and the Lawrence Systems YouTube page. I wrote this both as a way to learn and as an update to the Lawrence Systems video on ZeroTier for the Raspberry Pi as his original way is outdated.

# Download/Install Kali & Etcher

The first thing needing to be done (assuming you already have the necessary components to turn on and run a RP4) is to download the Kali Linux img.xz file to your computer. The link below will bring you to the Offensive Security download page; choose the img.xz file that fits the RPi that you have.

Kali Linux:

<https://www.offensive-security.com/kali-linux-arm-images/>

While you are doing that you’ll need a program that allows you to flash the img to the SD card. To do that I suggest Etcher. The link below will bring you to the download page. Once downloaded make sure to unpack (unzip) the file using something like winzip or 7zip

Etcher:

<https://www.balena.io/etcher/>

Now, the process of downloading Kali onto an SD card. An 8Gb SD card is required for any basic Kali usage. Insert the SD card into your computer then open up Etcher. From there click the Flash from File button and choose your Kali Distro. Select your target as the SD card (make sure there is nothing on it as everything will be deleted). Then click flash. Once finished, so long as there are no errors, this portion is finished.

# Running the RP4

At this point, if you haven’t already you’ll need to assemble your RP4. Follow the instructions from your point of purchase. Once you’re finished with that plug in your SD card and turn your RP4 on. Until we set up running headless, you will have to still need your RP4 connected to a display.

Once you boot up you’ll be presented with a login screen. Kali comes preset with a user on their RPi and virtual machine images. The username is [kali] and the password is [kali]. Log in and you’ll be presented with a login screen. Once logged in open a terminal to start setting up your RP4.

# Basic setup

In the last step we opened a terminal we need to work on a few things. The first has to deal with some basic security, we need to change the password for the user and root. You can do the same password for both, though realize that may be an issue if someone compromises your user account.

[side note: I don’t suggest changing the username for the base user. If you want to have a specific name create a new user and let that be your base account.]

In the terminal type the following:

passwd

press enter and you’ll be asked the current password. As you type nothing will show. Press enter and it will then prompt you to put in a new password for the current user. Once that is done type in:

sudo su

Press enter. You’ll be prompted to put in a password type in the new password you created for the user account. Type:

passwd

again you’ll be prompted like above for a new password. This is for the root account. For windows users this can be considered an administrator account. Type:

exit

which will bring you back to the normal user account in the terminal.

Next go to the top right, where the taskbar is, and connect to your internet. Once you’ve connected let’s update your Kali release.

We’ll be using the <https://www.kali.org/docs/general-use/updating-kali/> suggested process on this. You can click on the link or follow below.

We need to first make sure our source.list is correct. In the terminal type:

cd /etc/apt/

press enter and then type

ls -F

this will show the files in the current folder. Type:

cat /etc/apt/sources.list

this will display the text of the file in the terminal. You should have two lines of text in the file. If any are commented out with a #, type:

sudo nano /etc/apt/sources.list

this will open a terminal based text editor. Use your directional arrows to move to the line that has # and deleted the #. Press the CTRL button + x to exit. Press Y to save the file.

Lets go back to your home directory by typing:

cd

press enter and then type:

sudo apt update

press enter and this will update your package list which is where most updates received from. Next type

sudo apt full-upgrade -y

press enter and you will now update your packages and programs on your machine. This may take a while and it could have possible pop up messages which need your attention. This will vary by user.

At this point you have successfully installed Kali Linux onto your RP4, reconfigured the passwords for the user and root account, and updated your system to the latest releases. So long as you have no current issues with your RP4, let’s move on.

## Persistent Ip and headless operation

In order to access your RP4 from a secure shell (ssh), you must be on the same network. In order to do access your RP4 from anywhere and run basic commands from the command line, you’ll need to have a static IP address. For this we will be using ZeroTier, <https://www.zerotier.com/>.

ZeroTier is a free service that allows you to connect devices to a VPN which will then have a static IP address that you can then put on whatever device (including a phone) and connect to. We will set this up so the RP4 automatically connects to ZeroTier on startup.

First make a ZeroTier account and connect your main device to your new network. Due to the process of that, I will not be going over it in this guide. Once that account is made, you’ll need to download the ZeroTier file which we will install on the RP4. To download this go to

<https://download.zerotier.com/RELEASES/1.6.2/dist/debian/buster/zerotier-one_1.6.2-2_armel.deb>

this will download the file and save it somewhere easy to access. This file is downloaded as a .deb file and will need to be installed. For that we will use the tool gdebi. Type:

sudo apt install gdebi

once that is installed go to the location you saved the file using the cd command. Next type:

sudo gdebi <full path to file>

you will need the full path to the file ie. Sudo gdebi /home/zerotier-one\_1.6.2-2\_armel.deb

that ZeroTier should be installed and running, to check this type:  
zerotier-cli status

you should get a response similar to “200 <information ONLINE”. Now we have to connect to your ZeroTier network. In the terminal type:

zerotier-cli join <insert network id>

this should now have you connected to your network. If you are logged in on the ZeroTier website your page should refresh and show a new device attached to the network. To allow it you’ll have to check the box under the “auth” section. Once that is done the page will eventually refresh and show the device as active and it will now have a static IP address.

The last thing to set up for this is auto joining the network upon startup. To enable this, in the terminal type:

update-rc.d zerotier-one enable

once this is complete you can restart your RP4 by typing:

sudo shutdown -r now

which will restart your RP4. Check your ZeroTier interface and see if it is still connected once it boots up. Alternatively you can type:

zerotier-cli status

into the terminal and it should show a 200 response and say ONLINE we saw earlier.

The final step in this basic setup is setting up a headless configuration. This is a new feature in the RP4 which I assume is due to the dual HDMI ports. This is a two step process as we will need to force the RP4 to turn on if it doesn’t receive as display connection. Second, we will need to turn on auto-login and turn off the sleep function of the unit.

First to turn off the sleep and hibernation function right click on the battery icon in the top right. This will then show the option to go to the power settings. Change the settings to where it will never sleep or suspend.

Then open a terminal and type:

cd /etc/lightdm

sudo nano lightdm.conf

this will open a terminal based text editor where we can un-comment two lines under the [seat] heading. Find these two lines

#autologin-user=

#autologin-user-timeout=0

Delete the #’s from the lines and where it says

Autologin-user=

Type your username against the = ie.

autologin-user=kali

press CRTL + x to exit and press y to save. This is now the time where we see if everything still works. In the terminal type:

sudo shutdown

this will shutdown your RP4. Turn the direct power off and unplug your display cable from the RP4. Turn on the RP4 and see if your RP4 reconnects to the ZeroTier network. Alternatively you can open a SSH program such as PuTTY (or command prompt on windows) and type:

ssh [user]@[ZeroTier Ip]

if your RP4 connects, you should be prompted to accept the SSH key and type the password to the RP4 user account. If everything connected you should have a terminal that is connected to the RP4.

Thanks for making it this far. If you have any issues please reach out to me.

Resources

https://null-byte.wonderhowto.com/how-to/build-beginner-hacking-kit-with-raspberry-pi-3-model-b-0184144/

(don’t use this websites download link, it is out dated) https://www.lawrencesystems.com/how-to-access-a-raspberry-pi-running-kali-linux-anywhere-with-zerotier/

<https://zerotier.atlassian.net/wiki/spaces/SD/pages/29065282/Command+Line+Interface+zerotier-cli>

https://sdatic.com/auto-login-kali-linux-on-raspberry-pi/