8/15/24

By: Eddie Espino

For:

# Installation & Configuration Instructions for Kali 2024.2 on RPI4

# Topics Covered –

* Installation on RPI4
* Remote Access Configuration
  + SSH
  + VNC
  + IP Interface
* Wireless Configurations
  + Check Interface
  + Monitor Mode
  + Information Gathering
  + Capturing Encrypted Traffic
  + Viewing captured data

## Kali Linux 2024.2 32bit install on Raspberry Pi 4 model B

1. From your desktop click on this link  [kali.org](http://kali.org/)  to go to Kali index site. I encountered issues with the download link on the kali.org main site.

<https://old.kali.org/arm-images/kali-2024.2/kali-linux-2024.2-raspberry-pi-armhf.img.xz>

Check the SHA256 sum

on mac it is command = shasum -a 256 <filename>

Windows please follow this link for sha256 checksum <https://windowsreport.com/checksum-on-windows/>

should equal this

2984ff757f164d334b7c23d14171a55ebb6ba3f4389e09c82c9a98249749bbb6

for kali-linux-2024.2-raspberry-pi-armhf.img.xz

1. Setup the SD card reader with the SD for RPI on your desktop
2. Download and Open Raspberry Imager, select model pi 4, for the OS go to custom then point to the file downloaded, and select your SD for storage.
3. When complete, remove the card, insert into RPI and boot.
4. Log into Kali.

User: kali

Pass: kali

1. Change root password – open the terminal application and use the following command.
   1. sudo passwd root
2. Change Kali user password (used @ login screen) using terminal application use this command
   1. passwd kali

## Update & upgrade Kali to the last snapshot version

This should be completed at least once a month or before starting an engagement. To upgrade Kali Linux on a Raspberry Pi 4 using the latest snapshot, you can follow these steps:

1. Change the repository to the latest snapshot. If this is not the first boot of the system then you can skip this step and move to step 3:

You can modify the `/etc/apt/sources.list` to point to the snapshot repository. The snapshot repositories are typically used to provide a frozen version of the Kali repository at a specific point in time.

Edit the sources list:

*sudo nano /etc/apt/sources.list*

The default repository usually looks like this:

deb http://http.kali.org/kali kali-rolling main contrib non-free

Replace kali-rolling to kali-last-snapshot so it looks like this:

deb http://http.kali.org/kali kali-last-snapshot main contrib non-free

2. Update the package lists:

Start by updating your system's package list to ensure you have the latest information on the available packages.

*sudo apt update*

3. Upgrade the system:

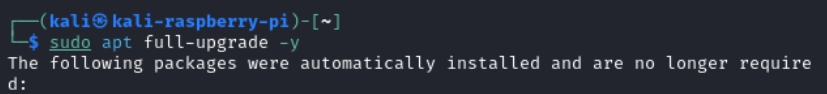
Once the sources list is updated, run the upgrade commands to update the system to the latest snapshot.

*sudo apt update*

*sudo apt upgrade -y*

*sudo apt full-upgrade -y*

4. If you receive the following message after the full-upgrade:



Then go ahead and run the command:

*Sudo apt auto-remove -y*

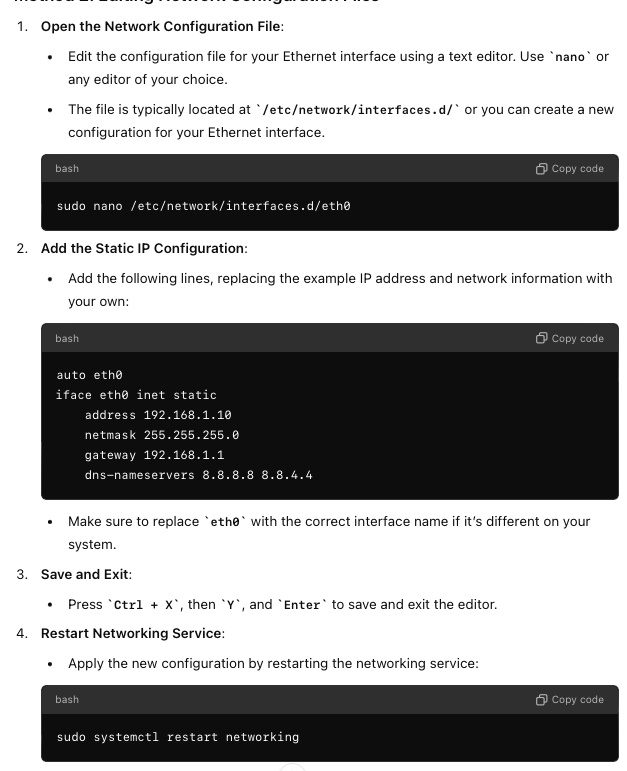
5. Reboot the system:

After the upgrade is complete, reboot your system to ensure all changes take effect.

*sudo reboot*

# Remote Control Setup for Raspberry Pi 4 with Kali Linux

# Assign a static address to the ethernet interface



Important

#### \*\* Please test that IP configuration survives after a reboot \*\*

## Enable SSH

Step 1: Open the terminal and enter into admin mode by issuing the following command. Once this command has been run you can omit prefixing *sudo* in next command in this document:

*Sudo su*

## 

## 

## Enable VNC

To start VNC server and create the password, you just need to use this command:  
*vncserver*

On the first run, you will be asked to provide a password (8 characters max). It will also give you the URL to access the session (infosec-kali:1 in my example).

**Warning**: the “8 characters max” information is important here.  
If you set “infosecscout” as your password, it will be truncated, so the real password will be “infosecs”. It’s not something we are used too in security (rather the other way around in general), so be careful.

Stop the current vncserver by issuing the following command

*vncserver kill :0*

Open the crontab with:

*crontab -e*

If prompted, choose your text editor for this (Nano is recommended)

Go to the end of the file and add this line:

*@reboot USER=kali /usr/bin/vncserver :1*

Try a reboot of the computer, VNC should now start automatically on display 0.

You can list the displays in using the following command

*ps -aux | grep vnc*

You will see a process for vncserver :# that number is the number of the display if it is not :0 then you can connect to the system <ip>:# where the number is the number of display seen in ps command.

# Connect to VNC

Download and install RealVNCViewer.

Connect to the ip

If it fails please check the displays for vncserver using the vncserver -list if it is on another display you can connect to it by appending the display number such as 10.1.0.234:1

# Backup you installation

To back up your Raspberry Pi running Kali Linux to a backup SD card, you can use the `dd` command on another Linux system or even on the Raspberry Pi itself. This process will create an exact copy (bit-for-bit) of the SD card, which can be restored later if needed. Here's how to do it:

\*\*What You'll Need\*\*

- A secondary SD card of equal or greater size than the one you want to back up.

- A USB SD card reader (if you're using the Raspberry Pi itself to perform the backup).

\*\*Steps to Backup:\*\*

1. Insert Both SD Cards:

- Insert the backup SD card into the USB SD card reader and connect it to the Raspberry Pi.

2. Identify the SD Cards:

- Run the following command to list the storage devices:

*lsblk*

- Identify the devices corresponding to your SD cards. Typically, they will appear as `/dev/mmcblk0` for the internal SD card and `/dev/sdX` (where X is a letter like `a`, `b`, etc.) for the backup SD card in the USB reader. Be \*\*very careful\*\* to correctly identify these devices to avoid data loss.

3. Backup Using `dd` Command:

- Use the `dd` command to create an image of the SD card you want to back up and write it directly to the backup SD card. Replace `/dev/mmcblk0` and `/dev/sdX` with your actual device paths.

*sudo dd if=/dev/mmcblk0 of=/dev/sdX bs=4M conv=*fsync status=progress

- `if` (input file) is the source SD card you want to back up.

- `of` (output file) is the destination SD card where the backup will be stored.

- `bs=4M` sets the block size to 4 megabytes, which generally speeds up the process.

- `conv=fsync` ensures data integrity by forcing all I/O operations to complete before moving on.

\*\*Note:\*\* This process might take some time depending on the size of the SD card.

4. Verify the Backup (Optional):

- After the backup is complete, you can compare the two SD cards to ensure the backup was successful:

*sudo cmp -n $(sudo blockdev --getsize64 /dev/mmcblk0) /dev/mmcblk0 /dev/sdX*

This command compares the two devices bit-for-bit up to the size of the source SD card.

5. Safely Remove the SD Cards:

Once the backup is complete, safely eject the SD card:

*sudo umount /dev/sdX*

*sudo eject /dev/sdX*

6. Verify the Backup by replacing the backup SD card with the running sd card to make sure you get a bootable system.

7. Store Your Backup SD Card:

- Label and store your backup SD card in a safe place.

# Wireless Interfaces Checks

Use the following to obtain interface information. Typically wlan0 is internal, and wlan1 is Alpha.

*ifconfig*

*iw list | more*

*iwconfig*

*iwlist <interface> <option ex: channel, txpower> -- iwlist to see all options*

*iw dev*

Check the supported modes (iwconfig) for monitor mode of the interfaces

Supported interface modes:

\* IBSS

\* managed

\* AP

\* AP/VLAN

\* monitor

\* mesh point

\* P2P-client

\* P2P-GO

\* outside context of a BSS

Check if an interface supports packet injection

aireplay-ng --test <interface name>

# Wireless Monitor Mode

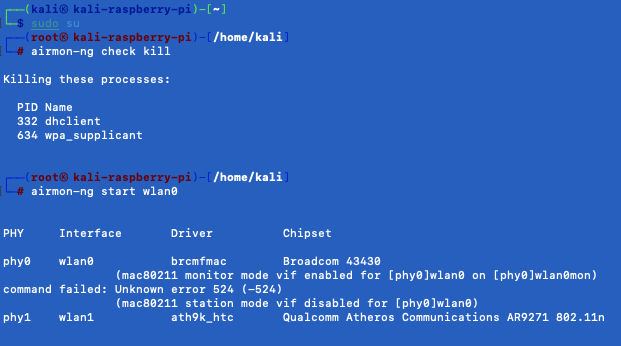
This would be for the internal interface for the packet captures

*sudo su*

*airmon-ng check kill*

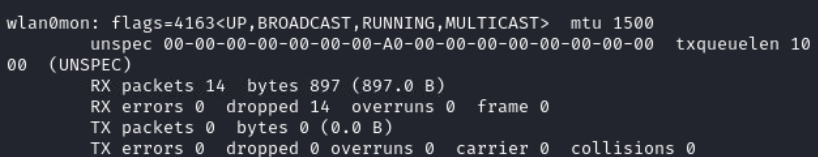
Now, we will set up the monitor interface. The errors shown below are typical. This can also be configured manually with the ifconfig & iwconfig commands as described under the deauth section.

*airmon-ng start wlan0*



Running iwconfig should show the monitor interface as wlan0mon.

*Iwconfig or ifconfig*

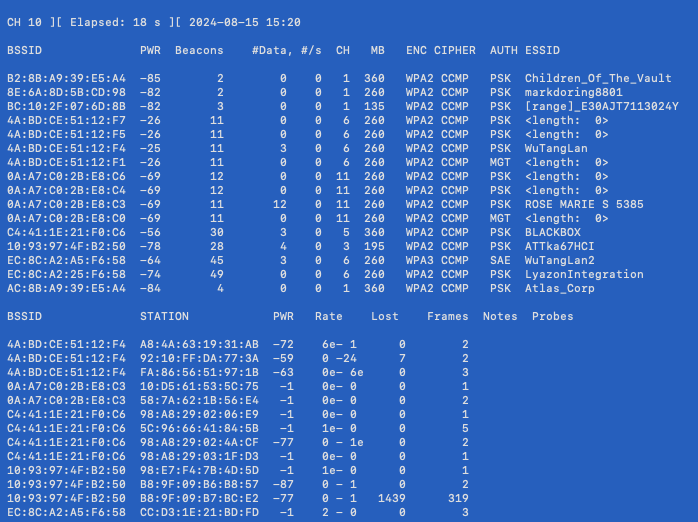


# Info Gathering

These commands are used to see the nearby access point their [BSSID], [ESSID] and their associating clients It is also necessary to note the Channel of your target SSID. This is all helpful information and should be recorded.

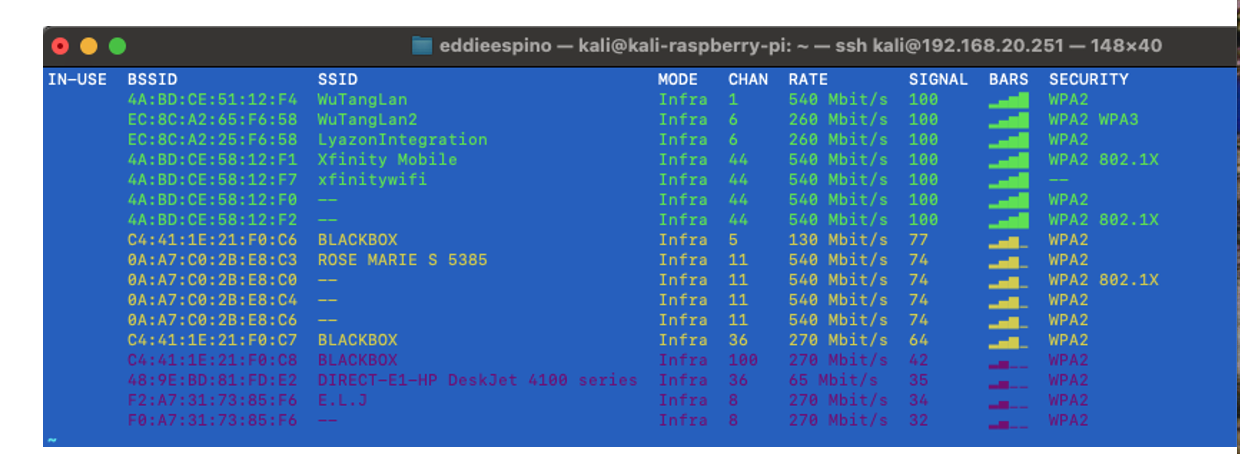
*sudo su*

*airodump-ng wlan0Mon*



Here is another way to display AP client info. This can only be used before using airman-ng kill command. See section “Reset for normal networking” below

*nmcli dev wifi*



# Capturing Encrypted

To capture the handshake for a machine, you will need to force the machine to (re-join) the network while the capture is in progress or have them connect to the wireless while capturing. One way to do this is to put the machine to sleep before you start the capture, start the capture, and then wake the machine up. Another way would be to deauth the client using an adaptor that supports packet injection. Command details for deauth are shown in upcoming section.

Command to check if an interface supports packet injection

*aireplay-ng –test <interface name>*

# Capturing Traffic

Capturing traffic can be accomplished using Wireshark or airodump command line interface which is listed below. There are many syntax options depending on what you want to capture. You capture just by channel number, SSID, BSSID, etc. The command below is the most common command you will need. Please find the channel number of the AP/BSSID using the commands from info gathering section above.

*airodump-ng --essid xxxx --channel <channel number> wlan0mon --write /tmp/<file-name>.pcap*

## Force Deauthorization of a device to capture the handshake:

\*\* Make sure the packet injection wifi interface (Alpha) is set to monitor mode with the correct channel you are targeting \*\*

### Set monitor mode and channel

*Sudo su*

*ifconfig wlan1 down*

*iwconfig wlan1 mode monitor*

*iwconfig wlan1 channel <channel number>*

*iwconfig wlan1 up*

### Deauth One Device

1. Identify the Target Device and AP:

1. Use `airodump-ng` to identify the target device's MAC address and the AP's MAC address.

2. Deauthenticate the Target Device:

Use `aireplay-ng` to deauthenticate the target device (replace the MAC addresses with the actual values). NOTE: --deauth 0 (continuous deauth), 1-10 (amount of deauth packets per client). Suggested value –deauth 5

sudo aireplay-ng --deauth 5 -a <BSSID> -c <TARGET\_MAC> <Alpha int wlan1>

### Deauth All associated and discovered devices on an Access Point

aireplay-ng –deauth 5 -a <BSSID> <name interface>

Stopping the capture & verifying pcap

Cancel the airodump command by using cntrl + c. Open the .pcap or .cap file in wireshark.

1. Check for Handshake Packets:

Use the filter `eapol` in Wireshark to verify you have captured the handshake packets.

2. Add the Decryption Key following these instructions:

<https://wiki.wireshark.org/HowToDecrypt802.11>

3. Analyze Decrypted Traffic:

After setting the decryption key, all encrypted traffic should be decrypted, and you should see all traffic, including unicast traffic between other devices.

Reset for normal for networking

When you are done tinkering in monitor mode and would like to use managed mode (normal networking) you should reboot Kali or do the following:

1. airmon-ng stop wlan0mon (or whatever the virtual interface name is)
2. service NetworkManager start
3. service wpa\_supplicant start
4. You may needs to use iwconfig to change back to managed mode of the alpha interface