COMP4337/9337 Securing Fixed and Wireless Network
Week 3 – Prep: Setting Up Your Gears

Due: N/A

Objectives

This preparation is intended to;

- set up your Raspberry Pi for the subsequent labs.
- familiarise the students with working on Raspberry Pi in a headless mode.

Note: This preparation should be carried out only after you receive the Raspberry Pi from the Teaching Assistants.

Overview

Raspberry Pi is a small single-board computer developed by the Raspberry Pi Foundation in association with Broadcom. Raspberry pi has gained popularity due to its low cost, modularity, and open design and has been widely used in many IoT projects, such as smart homes and robotics, including in building a portable penetration test tool.

As a computer, Raspberry Pi is usually equipped with a complete set of input and output devices, i.e., a monitor, keyboard, and mouse. However, Raspberry Pi can also be used without using any IO peripherals, i.e., called headless mode, in which, Raspberry Pi can still be remotely accessed and configured via SSH or Secure Shell.

In the subsequent labs and final project, you will be using Raspberry Pi in **a headless mode** to learn and explore several tasks in securing and hacking fixed and wireless networks.

Assessment and Marking

No deadline and no marks awarded for this preparation. However, you need to prepare your Raspberry Pi before starting Lab 2.

Flashing the image to the SD card

We have provided a custom image of Raspberry Pi OS (Raspbian Buster), in which some modifications have been made specifically for the COMP4337/9337 labs. Please follow these steps to flash the customised image to the provided SD card.

1. On your personal computer, download the customised Raspberry Pi OS image, `raspberry.img.gz` here. Make sure that you have an adequate internet connection as this process will download a Linux image of 4.5GB in size (approximately).
2. On your personal computer, download Balena etcher here, a tool to flash the downloaded image to an SD card.
3. Plug the SD card into your personal computer. Then open Balena Etcher to flash `raspberry.img.gz` to the SD card.
4. Select the appropriate image file and the SD card device on Balena Etcher. Click Flash to start flashing the image into the SD card.

5. Wait until the process is completed, and note that this may take several minutes. Upon completion, the SD card is ready to use and be plugged into the Raspberry Pi.

Connecting and accessing the Raspberry Pi

After plugging the SD card into the Raspberry Pi, you can connect to and access the Raspberry Pi by following these instructions:

1. Turn on the Raspberry Pi by connecting the Raspberry Pi to the power source via the provided power adapter. Please wait for a few minutes until the green LED have stopped rapidly blinking.
2. The Raspberry Pi will automatically start a wireless access point `testnetwork`. When prompted, please connect your personal computer to the network and type comp43379337 as the password.
3. Now that you are connected to the wireless network, you may access and control the Raspberry Pi remotely by connecting through SSH. You will need an SSH client already installed by default on Mac and Linux systems. For Windows, please install PuTTY to proceed. You may download PuTTY here.

   Note: You may want to check if your computer has been obtained an IP address from `192.168.4.0/24` address space.

4. Login to the Raspberry pi via SSH:

   For Mac and Linux systems

   Please open a new terminal window and type the following command to connect to the Raspberry Pi via SSH:

   ```
   $ ssh pi@192.168.4.1
   ```

   and type `comp43379337` as the password when prompted.

   For Windows systems

   Please open PuTTY, insert `192.168.4.1` in the Host Name field and `22` in the Port field, then click open on the bottom-right corner. When prompted, type `pi` as the username and `comp43379337` as the password.

5. A default bash console for Raspberry Pi OS should now be displayed. All the subsequent labs should be executed in this environment on Raspberry Pi.

Changing the SSID

Not necessary

Some of you may come to the booked rooms at UNSW to work together. It may result in a conflict, as all of you will have the same Access Point name (SSID) that may cause your personal computer to be connected to someone else's Raspberry Pi.

To avoid this conflict, you need to modify the SSID of your Raspberry Pi to a unique name. Follow these steps to change your SSID:

1. We have provided a shell script to simplify the process. The file is in `~/sfwn/wifi-setting.sh`.

2. Make sure you have connected to the Raspberry Pi via SSH, and type the following command from the home directory (~):

   ```
   $ sfwn/wifi-setting.sh reset <new-SSID>
   ```

   Please replace `<new-SSID>` with your desired SSID. Note that the script accepts alpha-numeric only; no whitespace allowed. For example:

   ```
   $ sfwn/wifi-setting.sh reset mynetwork4337
   ```

3. Your Raspberry Pi will be rebooted, and you will be disconnected from your current wireless network. You may close the terminal if it is not responding.
4. Wait for a few minutes, and you will find a new Wi-Fi network with the new SSID. Note that the password remains the same, `comp43379337`. You may now try to connect to the new network.
5. You can repeat this process if you wish to change the SSID later on.

Shutting Down the Raspberry Pi

It is a good practice to shut down your Raspberry Pi before plugging off the power cable. To shut down the Pi, you can type the following command:

```
$ sudo shutdown now
```

The console may ask for your password; please type `comp43379337`.

After the green LED stops flashing, you may now remove the power cable safely.