



Fleming College

IoT Scanner by ASA

Guide and User Manual

Thanks for using our IoT Scanner!

Before running the scan, please take a few minutes to read the user manual.

Contents:

1. General Information

- 1.1 Introduction
- 1.2 Why IoT Scanner?
- 1.3 Why Our IoT Scanner?

2. Getting started

- 2.1 Requirements
- 2.2 The Raspberry Pi
- 2.3 Connecting the SD Card
- 2.4 Connecting the Display
- 2.5 Connecting the Keyboard and the Mouse
- 2.6 Power On the Raspberry Pi
- 2.7 Running the Setup file

3. Step-by-Step instructions

- 3.1 `setup.sh` file
- 3.2 Changing the permissions
- 3.3 Running the `setup.sh` file
- 3.4 Scanning results
- 3.5 The GUI app
- 3.6 The Email App
- 3.7 Checking your results

4. Next Version and Updates

- 4.1 How to update?
- 4.2 What's coming?

5. Summary

1- General Information

1.1 Introduction

The Internet of Things or IoT is influencing our lifestyle from the way we react to the way we behave. From air conditioners that you can control with your smartphone to Smart Cars providing the shortest route or your Smartwatch which is tracking your daily activities. IoT is a giant network with connected devices. These devices gather and share data about how they are used and the environment in which they are operated.

1.2 Why IoT Scanner?

Anybody who is concerned with WIFI security and personal computer/laptop. For Example, Fleming college, McDonald's, Tim Horton, hotels, and home network. The IoT Tester can help scan the network you are connected to and list all vulnerabilities so we can be protected and detect any potential threat. This device offers detailed information (name, range, IP address, etc.) of all connected devices with detected vulnerabilities by checking and comparing from the in-built database.

1.3 Why Our IoT Scanner?

What makes this tester superior to most others on the market is its ability to detect Bluetooth devices not just devices on Wi-Fi networks. This tester will be connected to your system and performance will depend on your system specification.

Features:

Easy use - Nice and Simple graphical user interface - Fast responsive execution - Deliver results via email.

2- Getting started

2.1 Requirements

You need to have either a Raspberry Pi handed by us OR a setup.sh file That you can download from Dropbox. ([Link is Below at 3.1](#)).

- If you get the Raspberry Pi from us, all you need to do is to connect the Raspberry Pi to the Wi-Fi.
 - o On the upper right corner CLICK the Wi-Fi symbol > Choose your Wi-Fi network > Type your Wi-Fi password.
 - o You will see a file called “setup.sh” on your Desktop that is ready to run. DOUBLE CLICK the file > Execute OR Execute in Terminal.
- If you have your own Raspberry Pi, you can skip a few steps and go to ([3.1](#)).

2.2 The Raspberry Pi

In order to use the Raspberry Pi computer, you need the following accessories:

- A power adapter (included).
- SD Card (included and configured).
- A computer monitor, or television. Most should work as a display for the Raspberry Pi, but for best results, you should use a display with HDMI input. You’ll also need an appropriate display cable, to connect your monitor to your Raspberry Pi.
- A computer keyboard and mouse

- Any standard USB keyboard and mouse will work with your Raspberry Pi.
- Wireless keyboards and mice will work if already paired.

[Raspberry Pi Documentation - Getting Started](#)

2.3 Connecting the SD Card

Raspberry Pi computers use a micro-SD card, except for very early models which use a full-sized SD card. This card (64GB) will be included and configured for users, so they don't have to install an operating system.

2.4 Connecting the Display

Your Raspberry Pi has an HDMI port which you can connect directly to a monitor or TV with an HDMI cable. This is the easiest solution; some modern monitors and TVs have HDMI ports, some do not, but there are other options. (We will include the HDMI cable with the Raspberry Pi).

2.5 Connecting the Keyboard and the Mouse

You will be receiving a Raspberry Pi 4 Model B that has 2x USB 3.0 AND 2x USB 2.0 ports. Connect your keyboard and mouse to two of them.

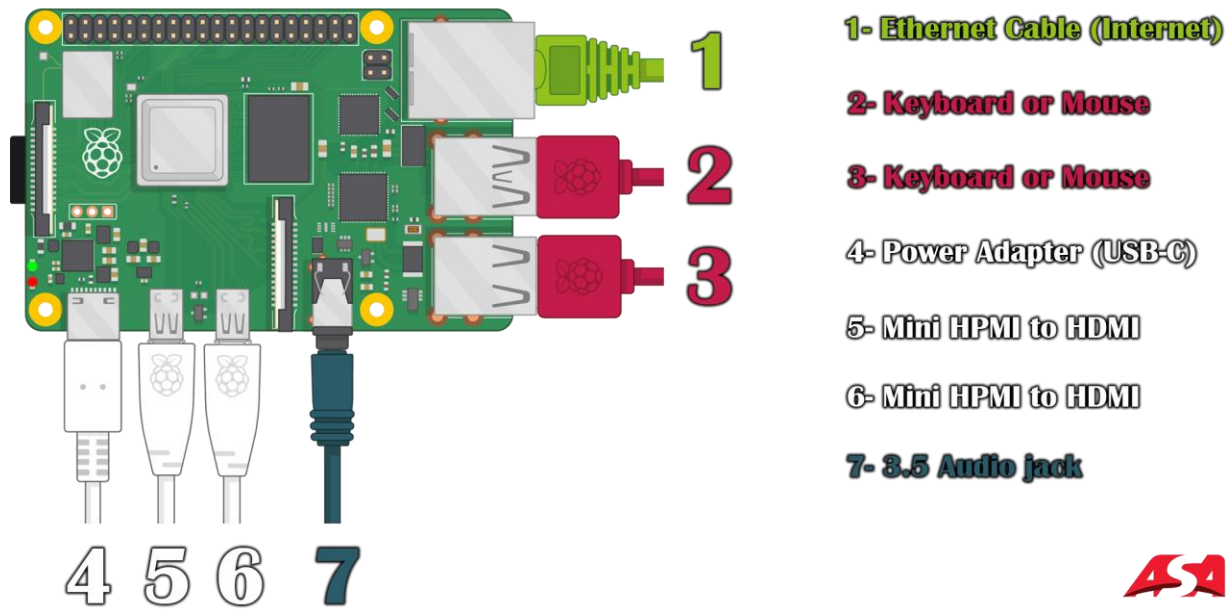


Figure 1: Picture from <https://www.raspberrypi.com/software/> Edited by ASA team

2.6 Power On the Raspberry Pi

After connecting the accessories, connect the power supply and the Raspberry Pi will start automatically (There is no POWER ON/OFF on the Raspberry Pi). Then, you will be logged in to the machine and directed to the Desktop.

2.7 Running the Setup file

After powering on the machine, you will see our setup file on the desktop. Don't run it yet. You can skip a few steps and go directly to [\(3.3\)](#).

3- Step-by-Step instructions

You can either watch the video to see how it's done OR follow the instructions below.

Video Link: <https://youtu.be/6sr7vAXrZN4>

3.1 setup.sh file

The user needs to have our file "setup.sh". When running this file for the first time, it will install the latest system update (update the packages), Python3, Python-pip3, and some Python modules required to complete the scan and run our app. The modules include Tkinter (used for the GUI), Bluetooth (to scan for Bluetooth devices), and nvdlib (to get info about vulnerabilities and CVEs from the NVD Library).

You can download the file from the following link:

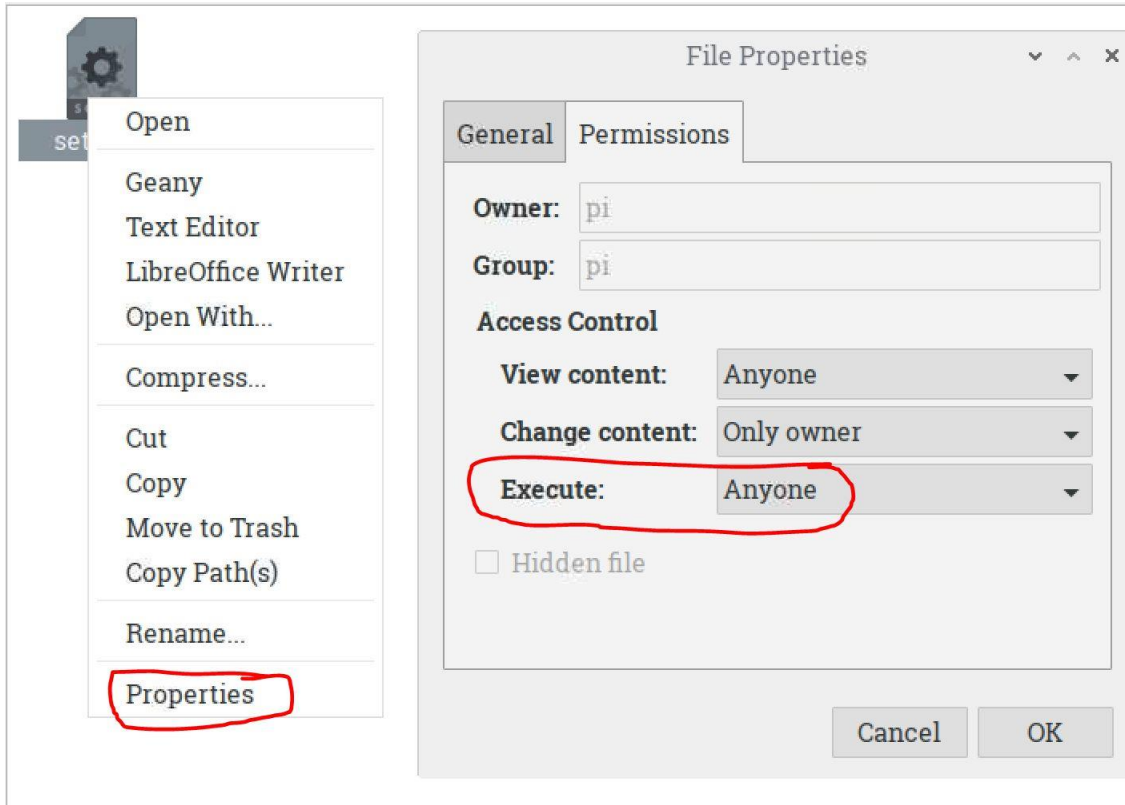
<https://www.dropbox.com/s/2kilsloe52vm8xp/setup.sh?dl=0>

3.2 Changing the permissions

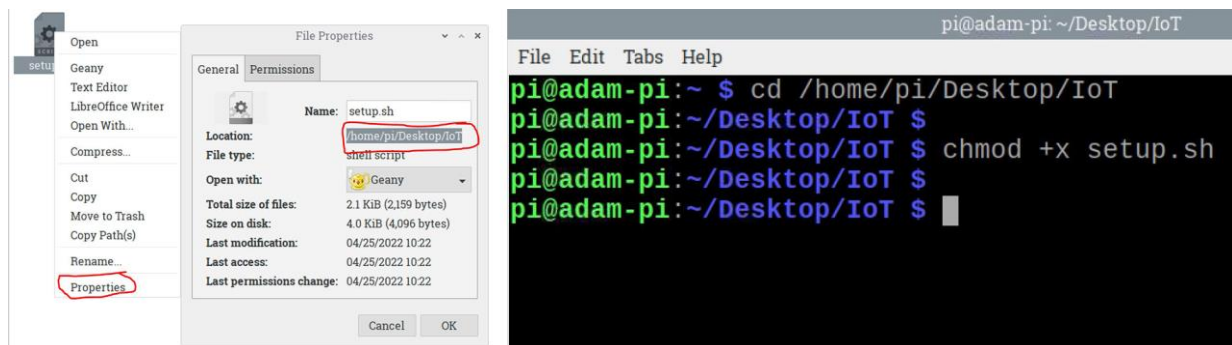
After downloading the setup.sh file, you will need to change the "Execute permissions" to anyone so you can run the file in your machine.

There are two ways to change the permissions (The first way is much easier):

- 1- Right Click the file (setup.sh) > Properties > Go to Permissions tab > Change "Execute" to "Anyone". As shown on the next picture:



- 2- Right Click the file (setup.sh) > Properties > Under General > Copy the location of the file (path) > On the top left corner or down left corner > Click your Raspberry Pi logo > Choose "Accessories" > Terminal > Type without brackets (cd AND_THEN_PASTE_THE_COPIED_LOCATION) > Hit Enter
- > Now type without brackets (chmod +x setup.sh) > Hit Enter



To run the Terminal, Click the Raspberry Pi symbol at the upper left corner > Accessories > Terminal

3.3 Running the setup.sh file

You can either watch the video to see how it's done OR follow the instructions below.

Video Link: <https://youtu.be/6sr7vAXrZN4>

Now, you can run the setup file.

Double click the setup.sh file and then choose either Execute OR Execute in Terminal.

3.4 Scanning results

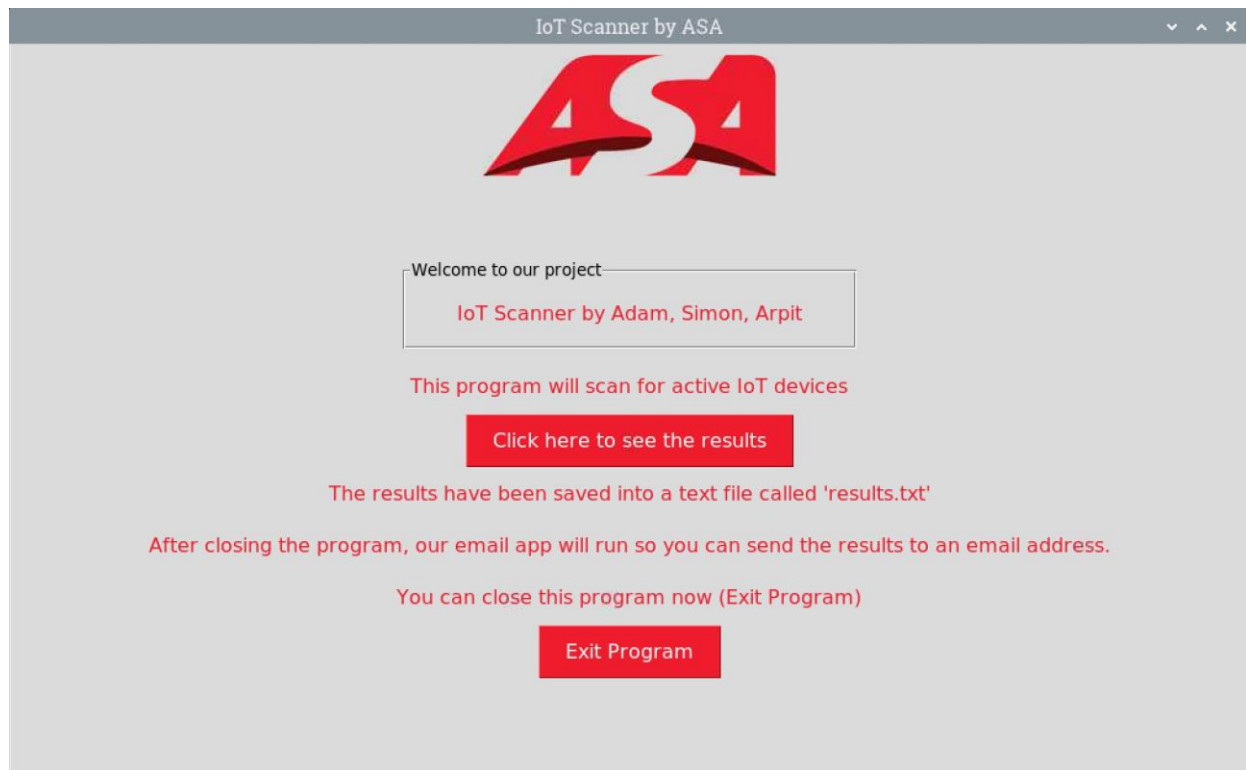
After running the setup.sh file, if you choose “Execute in Terminal”, you will see that the scan is started, and it will show your connected devices with their IP and Mac Addresses. Wait for a few minutes till the GUI starts.

NOTE: It might take 5-10 minutes before the GUI starts.

3.5 The GUI app

When the completes, our GUI app will start. We’ve made it so simple, so the end users know how to use it.

You will see only 2 buttons on our GUI app. The first one is to see the scanning results in a good and an understandable format, and the second button is to exit the program.



When you click “Click here to see the results”, a second window will open, so you can get full results. You can select all the results, copy them, and paste them in a text file. BUT we’ve made easier for the users. Our tool will save the results in two separate files. The first file named “rev.txt” that would contain a list of all the connected devices with their names, IP addresses, and Mac addresses, and the second file named “results.txt” which is the most important one. It would contain a list of all vulnerable devices with their product names and CVEs.

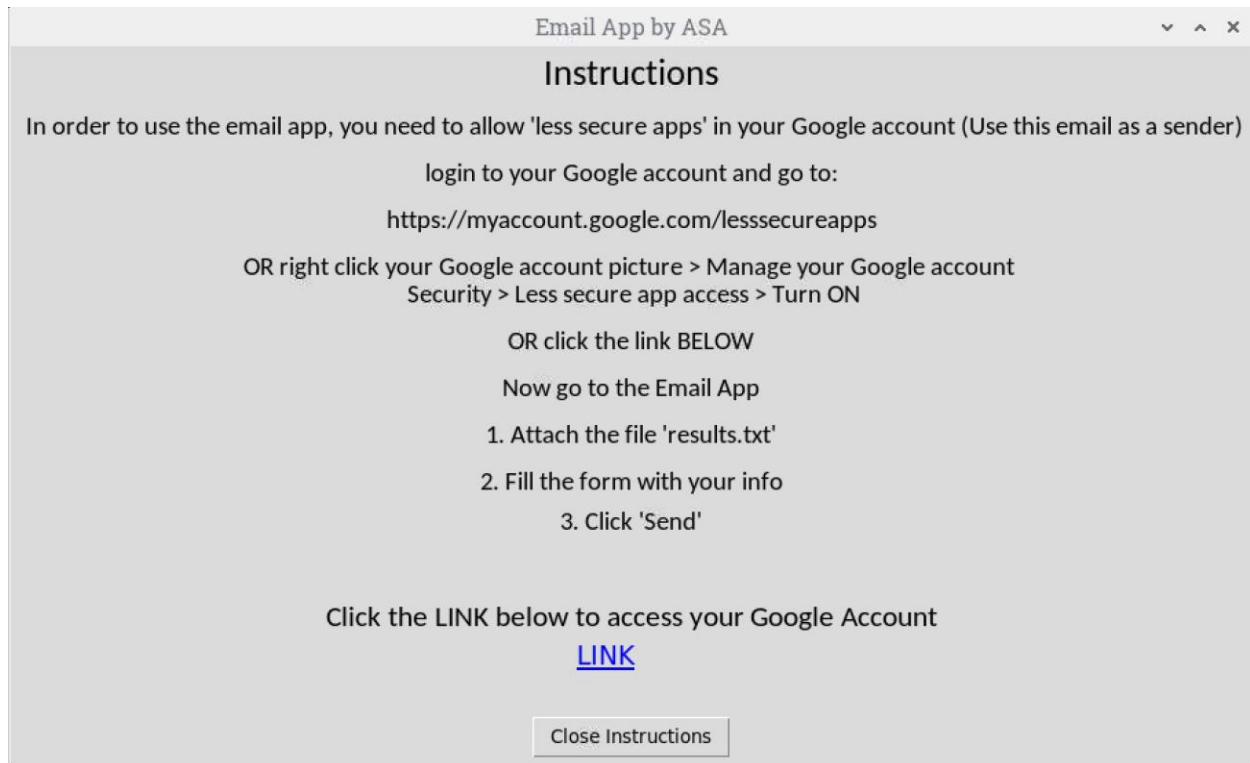
Now, you can close the program by clicking “Exit Program” button.

3.6 The Email App

When you close the program, our email app will start. You will get two windows.

The first window is the instructions in how to send an email using our email app, and the second window is the email app as show on the pictures below.

You can follow the instructions on the second window or complete them here.



- To be able to send emails via this app, you need to TURN ON "less secure apps" on your Google account.

This is required because our email app was created using Python and Python is considered a third-party app.

- Go to the following link <https://myaccount.google.com/lesssecureapps>
- Sign into your Google Account.
- Turn the option ON (Which should be OFF by default).
- Go back to the email app.

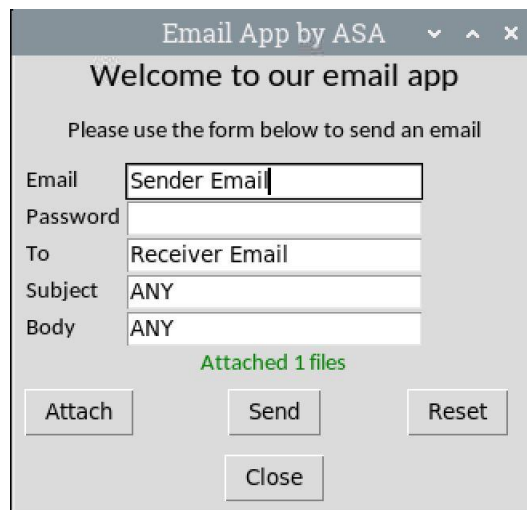
We recommend going back to <https://myaccount.google.com/lesssecureapps> and turning "less secure apps" OFF after sending the email.

Our next version v2.0 will not ask the user to enter the "sender email address". Users will have to enter the "receiver email address" only.

- Close the Instructions window and go back to the email app.
- Fill out the form with your info
 - o Email: The Google account that you used in the previous step.
 - o Password: The same Google account password.
 - o To: The email address you are sending the file to.
 - o Subject: Any
 - o Body: Any
- Click "Attach" and select the file "results.txt".

You may wish to attach a file called "rev.txt". This file contains a list of all connected devices.

- Click "Send"



The screenshot shows a window titled "Email App by ASA" with a close button. Inside, it says "Welcome to our email app" and "Please use the form below to send an email". The form has five input fields: "Email" (containing "Sender Email"), "Password" (empty), "To" (containing "Receiver Email"), "Subject" (containing "ANY"), and "Body" (containing "ANY"). Below the fields, it says "Attached 1 files" in green. At the bottom, there are four buttons: "Attach", "Send", "Reset", and "Close".

3.7 Checking your results

Go to the email address that you sent the file to > Open the email you received > Click the attached file/files > The file "results.txt" contains all the vulnerabilities associated with your devices.

You can copy one of these CVEs and search for them on Google or NATIONAL VULNERABILITY DATABASE (NVD) at <https://nvd.nist.gov/>

THE NATIONAL VULNERABILITY DATABASE contains a list of all CVEs. Each CVE includes Details/Description, Severity, Solutions, and more. You can follow the solutions to secure that device.

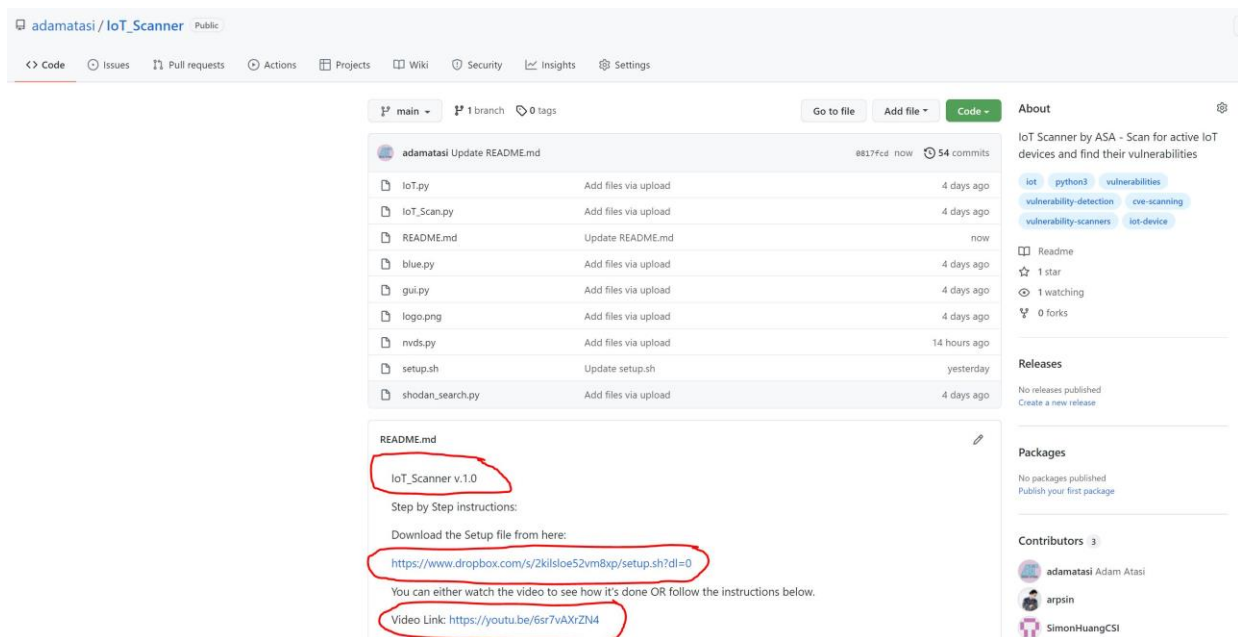
4- Next Version and Updates:

4.1 How to update?

In order to keep following the latest updates of our IoT Scanner, you need to follow the scanner page on GitHub at https://github.com/adamatasi/IoT_Scanner

We will keep pushing updates to make sure that our tool never expires.

What users need to do is to go to our scanner page, scroll down, and check the README file as shown on the next picture:



Check the version of the scanner. This is version 1.0 (v.1.0). If there is a new update, we will post the new version on that page and change that to something like “v.1.1” or “v.2.0”.

We will also upload the file to a cloud storage and give the link as well as a new video instruction.

If we were to make big changes, we would most likely make a new user manual and post it on the same page.

4.2 What's coming?

Our next version of the scanner will include:

- Better email delivery method so users don't have to turn on "less secure apps" on their Google Accounts.
- Better GUI looking app with more buttons so users can choose where to save the results.
- Better results: That includes more details about each CVE and solutions.
- Our next version will support Windows machines as well as Linux machines running on Virtual environments.
- We might add some links to each vulnerability detected on each device to help you secure your network, that includes, YouTube videos, articles, and more.

5- Summary:

Scans the network and lists all device IP addresses and MAC addresses. It will then allow the user to select a device and will be able to track this device's detailed info This could help make the network more secure and be aware of potential threats.

The main objective is to map out the IoT devices and their associated vulnerability.

List all networks Wi-Fi and Bluetooth devices with name and IP address

Compare scanned results for vulnerabilities by looking into the database

We used python3 to create scripts and execute them to achieve the goal

First, we divided the project into parts so we can work on it individually which would be

1. Execution script.
2. Scanning network script Wi-Fi and Bluetooth.
3. Database to store scanned results.
4. Scanning vulnerabilities with NVD.
5. Result email delivery.