

# Who Is Home?: Network Scanner

Marc Geggan

BSc (Hons) Ethical Hacking: CMP408

## Introduction

This project is a proof of concept for access control that utilizes a Raspberry Pi Zero to monitor a home network for specific IP addresses in order to detect connected devices and individuals. The Pi runs NMAP scans locally and transmits the data to an AWS EC2 instance via MQTT for display on a static web page. The network scanner is capable of detecting the connection and disconnection of specific devices, with a focus on mobile device IP addresses, and logging times, dates, and the number of individuals present in the home. This concept can be utilized to track the comings and goings of individuals through their connection of devices to the network.

The primary objectives of the IoT aspect of this project include:

- Running a Python script to scan the network every 10 seconds for specific devices
- Publishing data to the EC2 instance via MQTT messages
- Utilizing a backend Python script on the EC2 instance to convert MQTT messages into an HTML file
- Displaying a table of information and logs of devices on the network via a static web page.

The primary objectives of the hardware aspect of this project include:

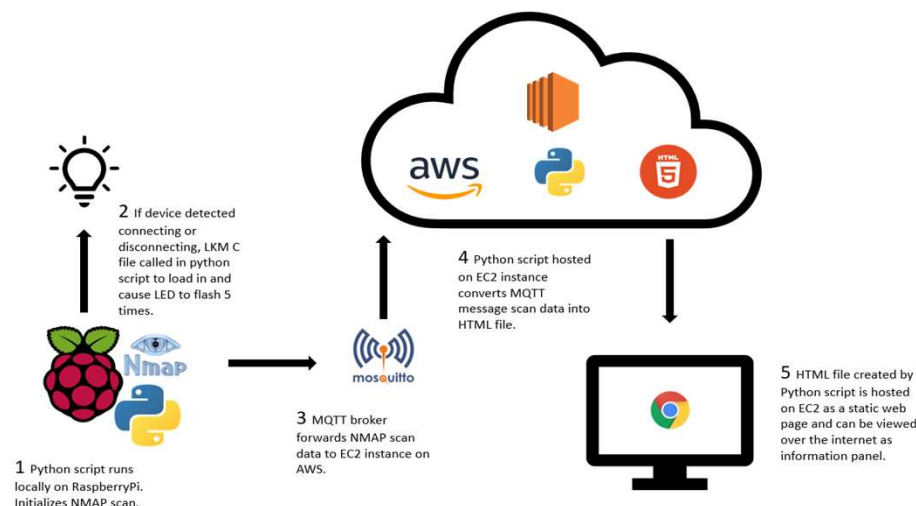
- Utilizing GPIO pins and a Linux Kernel Module (LKM) to flash an alerting LED light
- When a device joins or leaves the network, the LKM C script is called, and an LED will flash 5 times.

## Methodology

This project utilizes Python scripts to conduct network scans, invoke the Linux Kernel Module (LKM), and establish communication with the cloud via the MQTT protocol. The Python programming was divided into two separate files, a frontend and a backend. The frontend, hosted locally on a RaspberryPi device, is responsible for tasks such as nmap scans, MQTT messaging, and LKM invocation. On the other hand, the backend, which is stored on an Amazon Elastic Compute Cloud (EC2) instance, is responsible for converting MQTT data into an HTML file and saving it to the `"var/www/html"` directory for internet-based viewing.

During the creation of the EC2 instance, it was observed that each instance initiation results in the assignment of a new IP address. This necessitates the modification of certain variables within both the frontend and backend scripts prior to their execution. Specifically, the variable `"broker_url"` in both scripts must be updated with the newly assigned IP address of the EC2 instance to ensure successful MQTT connectivity. To view the messages being sent, the EC2 IP address must also be added to MQTT message software, in this case, `"MQTT Explorer"`.

Once the necessary updates have been made, the `"Mosquitto"` MQTT broker can be run in the background on the EC2 instance. The frontend script can then be executed on the RaspberryPi device, while the backend script is run on the EC2 instance. To access the webpage, the IP address of the EC2 instance must be entered into the web browser, and the page will load upon completion. A diagrammatic overview of the project architecture is provided for reference.



## Project Highlights

Overall, the project worked as planned and incorporated software, hardware, and cloud to create a successful IoT network device scanner that publishes data to a website hosted on the cloud, with visual hardware LED alerts.

Highlights of this project include:

- Customizable users and devices to be scanned for over network.
- Fully documented code for easy software modification and future work.
- Automated network scanning and publishing to cloud services.
- Easily viewable scan results presented on a web page.

## Future Work

- Enabling the use of static MAC addresses of devices will allow for more stable results.
- Utilize databases to store times and dates of devices interacting with the network.
- Use more information from NMAP scan results to display more metrics on the devices attached to the network.

## References

[www.linkedin.com. \(2021\). Host a static website on AWS EC2. \[online\] Available at: https://www.linkedin.com/pulse/host-static-website-aws-ec2-chandan-mishra?trk=articles\\_directory](https://www.linkedin.com/pulse/host-static-website-aws-ec2-chandan-mishra?trk=articles_directory) : Cope, S. (2019). *Beginners Guide To The Paho MQTT Python Client*. [online] *Stevens-internet-guide.com*. Available at: <http://www.stevens-internet-guide.com/into-mqtt-python-client/>.