We found that IoT devices are usually unsecure. They allow any user on the same local network Wi-Fi to control them. They never ask for any login information.

We researched IoT devices attacks and found an article on DoS attacking a Sonos Device.

We watch many videos on “how to” DoS attack a Sonos Device.

We determined that in order to perform a DoS attack we would need a Sonos Device application that could write the code and perform the action. Since we already had a Sonos Device all we needed to do was download the software and applications.

After doing some research we found that the API for many standard IoT devices are well known and documented unofficially. The Sonos API has a library for Python.

After doing research we found that a program called PyCharm would be the best environment to write our code and execute the attack.

How to take control of a sonos

<https://null-byte.wonderhowto.com/how-to/take-control-sonos-iot-devices-with-python-0191144/>

Soco Library

<https://docs.python-soco.com/en/latest/>

Calculating Subnet

<https://www.baeldung.com/cs/get-ip-range-from-subnet-mask>

What are IoT devices

<https://www.techtarget.com/iotagenda/definition/IoT-device>

Configure your firewall to work with sonos

<https://support.sonos.com/en-us/article/configure-your-firewall-to-work-with-sonos>

Millions of Roku and Sonos Devices Easily Hacked: What to Do

<https://www.tomsguide.com/us/roku-sonos-dns-rebinding-attack,news-27485.html>

Pycharm

<https://www.jetbrains.com/pycharm/>

Python

<https://www.python.org/downloads/>

chatGPT