



# IoT NETWORK SCANNING COMMAND LINE TOOL

ASHLYN COOPER AND KAITLYN PIERCE

CPSC 4240 – DR. DRACHOVA

# PROJECT OVERVIEW

- We created a command line tool that allows users to view the IoT (Internet of Things) devices connected to their network based on a user-selected type of scan
- This tool builds off *nmap* but aims to be more user-friendly by providing the user with detailed explanations of the various types of summary reports that can be generated
- Through this, users do not need to memorize *nmap* flags or their IP address and can instead input the character input that corresponds with their desired report

# NMAP

- *nmap* (Network Mapper) is a free and open source utility for network discovery and auditing
- Supports dozens of advanced techniques for mapping networks
- Documentation and reference guide can be daunting and hard to find exactly what options you want to use if you are a novice



# PROJECT MOTIVATION

- **Tool Goal:** To develop and implement a user-friendly program that scans, analyzes, and outputs the IoT devices connected to a specified network in our Ubuntu Linux environment.
- **Tool Relevance:** Due to the prominence of IoT devices and the increasing risk of cyber-attacks, this tool can assist all computer users in protecting their networks. The ease-of-use and condensed network information would be helpful for less experienced users to utilize on their networks for threat analysis.



# PROJECT DEMO

<https://github.com/kjpierc/4240-CLT-project>

