# Research

Python language may be used for it’s ease of interfacing with the underlying tools

Tkinter may be used to implement a GUI for the user, provides a simple interface. PyQT may also be used

Nmap for scanning network, multiple python libraries for it exists, can be used to find devices on network and identify OS type, OS version and device type

Devices on my home network:

* 4 LG Smart TVs
* 1 Lenovo Laptop
* 2 Brother Printers
* 1 HP Printer
* 1 Desktop PC
* 2 Thinkpad Laptops
* 1 Android Phone
* 1 Sky TV box
* 4 IPhones

Devices on friend’s network:

* 1 Smart TV
* 2 IPhones
* 1 PS5
* 1 Asus laptop

Network Discovery by runZero is a similar program( https://www.runzero.com/topics/network-discovery/ )

## Nmap Sources:

<https://nmap.org/book/toc.html> (Offical nmap guidebook online version is free but with half the content of print ver.)

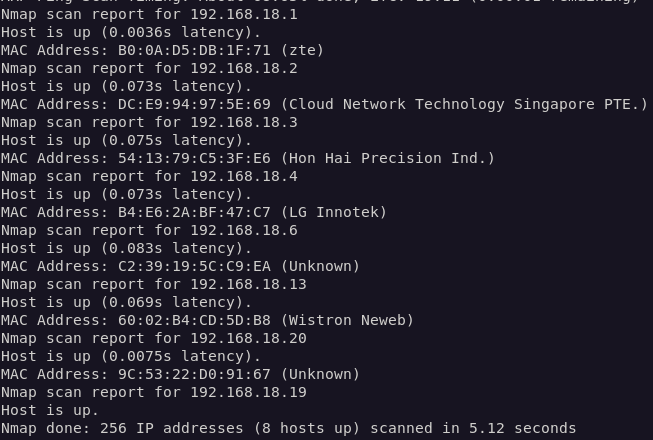
<https://www.stationx.net/nmap-cheat-sheet/> (Nmap cheat sheet of most useful commands)

<https://wiki.archlinux.org/title/Nmap> (Arch wiki page on Nmap)

## Nmap Commands:

-Oa <filename> : output results as xml, grep and normal file

nmap –sP <target> : Basic ping scan



nmap -O -osscan-guess <target> : Scan aggresively for detailed OS info



Nmap —top-ports <number> <target> : Scans for the top <number> most used ports

Nmap –sV –A —version-all <target> : Scan for services, their versions and details

