# Future Work

The overall purpose of this program is for it to identify potential information in the current network that could be useful to an attacker, hence ensuring that this network has no vulnerabilities, and that a new smart device would be safe to join it. This means this program has much use, and can be improved more, helping the end user to an even higher extent.

More information being outputted to the user could help the system be of more use. A piece of information which “Angry IP scanner” (another publicly available port scanner) outputs that I thought could be quite useful is the ping speed, in m/s, of each device it finds. The ping of a device is the speed it takes for a message to be sent from the originating host to the device computer, in effect testing the reachability of the host. It could be useful for a user of our program to know this so that they know how well connected each device is to the network.

Another possible improvement of the current system would be for it to have the ability to scan for more specific ports. There are many different ways in which the system could be adapted to search for different IP addresses in particular. We could give the user the option to input a single IP address, a range of IP addresses (searching from the start to the end of the list), or even read in addresses from a text file, which could potentially help improve the scalability of the program.

One point that could be improved about the system in its current state is the time it takes to do the search, in particular the device scanner. As it stands the Jar file goes into a “not responding” state for a few seconds before presenting the information to the user, which isn’t ideal for the end user. A quicker method of doing these searches could help improve the system for the user, potentially through the use of threads.

Adding UDP port scan functionality would be another useful extension to the program. This would not be easy due to the nature of UDP being connectionless, so as a result would not be able to be detected in the same way TCP packets are. However, this can still be possible by using application-specific UDP packets to get a response.

As it stands the system can save to a text file and can be encrypted. An extension to this feature could be for as well as it being able to be saved to a text file, the results could also be saved to a database. This could be done using JDBC (Java Database Connectivity), which can establish a connection with an SQL database, and be used to export the result from the searches.