Is it possible to identify the tool used to scan an ICS device by analysing the traffic received?

There are many tools available to inspect and analyse ICS assets. Attackers use these tools during reconnaissance before they begin attacking. There are several vectors which may indicate that a scan is malicious, including time, intensity, source address, and using the wrong tool. Each of these parts in isolation would not provide sufficient and sound intrusion detection, but may do if combined together.

The aim of this project is to analyse the packets received by an ICS device during a scan, and identify which tool is being used. This is only part of the puzzle, but will prove useful in ID systems. We will also investigate what can be done to obfuscate which scanner is being used, in order to fool our classifier.

Identify which tools are used (nmap, plcscan)

* Luckily a grad has done this bit

Understand how they work

* Look at source code
* Look at packets received
* Read up on protocols like Modbus

Test between two tools

* If there is a difference, test more
* Some may turn out to be the same

Build classifier

Work out what can be done to confuse the analysis.