Investigating the viability of toolset detection within OT network scanning, providing another indicative vector to use in IDS.

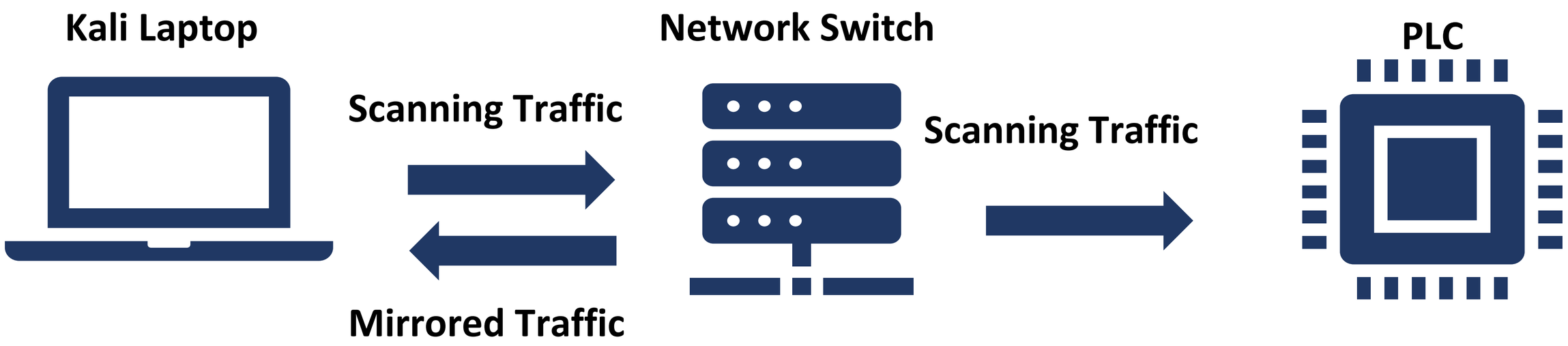
Introduction

There are many tools available for engineers and admins to inspect and analyse OT (operational technology) assets on their networks. 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.

The aim of this project is to analyse the traffic received by an ICS device during a scan, and identify which tool is being used. This could be used as a vector in IDS. We may also investigate what can be done to obfuscate which scanner is being used, in order to fool our classifier.

Method

I will use a laptop running Kali to launch the scans against the S7 1200 PLC testbed over ethernet, shown in the diagram below.



For detection, I have settled on 3 methods:

- **Number of packets** – very basic, there will be variation in the versions of tools used so not particularly effective
- **Bandwidth analysis** – noisy
- **Packet content** - It may be that certain tools send certain packets in a specific order or only send certain packets

University of BRISTOL

Zack Dove
zd17646