Localised Internet Scanning Infrastructure

Student: Jordan Myers

Supervisor: Dr. Stephen Farrell

Degree: Integrated Computer Science

Year: 2019

Internet scanning is used for a variety of purposes, some good and some bad. Researchers and commercial entities use Internet scanning to find new vulnerabilities, monitor the roll out of mitigations, uncover unadvertised services such as Tor bridges and perform high-speed vulnerability scanning. Attackers use it to find new vulnerabilities and targets with known vulnerabilities.

Internet-wide scanning is a well-explored topic but more localised scanning could produce more actionable results. This project implements a data store and data visualisation tool for such scans. It explains how Elasticsearch was configured to store scan results and describes a CLI tool developed to simplify the process of working with Elasticsearch. It explains how Kibana was used to visualise the data in Elasticsearch and provides some high-level analysis of the data from three scans. Finally, it highlights the strengths and limitations of using the Elastic Stack as part of a localised Internet scanning infrastructure.