Project Number: 19

Project Title: Automated E8 Compliance and Remediation

Project Clients: Jesse Laeuchli, Arash Shaghaghi

Project specializations: Software Development;Web Application Development;Big data Analytics and Visualization;Cloud Computing;Computer Hardware and Networks;Security/Cyber Security;

Number of groups: 3 groups

Main contact: Jesse Laeuchli, Arash Shaghaghi

Background:

Compliance with security standards is an important goal in cyber security. We are interested in developing software that can be used to automate compliance with ASD's essential 8.

Requirements and Scope:

The project would aim to develop a set of tools which would

1). Collect data about the state of the clients network and hosts

2). Analyse the collected data in order to determine compliance level, based on the ASD checklist.

3). Provide the results in the form of a dashboard. We have a dashboard which reports compliance of other standards, so integration with this dashboard would be ideal.

4).Where appropriate the tool would seek to remediate lack of compliance.

Required Knowledge and skills:

The project has three main parts

1). Development of a data collection application which can be deployed to clients and servers, which would read different system options and configurations, as well as different network options and configurations. This application would collect the data required to determine if E8 is being met at a given maturity level. This requires reading many configuration settings at the system and network level, and would need to make extensive use of system APIs and Powershell to obtain this information.

2). A server application which will manage the deployed data collection clients, and then use the collected data to determine if the network meets a given control at a given maturity

level. This application could be written in anything, but will require some understanding of networking as well as general software development skills.

3). A web dashboard, where the results can be displayed. This dashboard could be stand alone, but ideally would integrate with our existing dashboard. This will require an understanding of web application development.

Expected outcomes/deliverables:

Source code, and a deployment guide.