CYB333 Security Automation

Course Project

Daniel T. Nguyen

October 24, 2020

Project Plan and Scope

This project is aimed at allowing technicians the ability to query for registry keys within a specified root registry hive. The purpose is to provide a list of registry keys that can be passed to analysts for further investigation. A scenario in which a registry key list needs to be queried and validated, is in the case where an incident has occurred involving creation of new registry keys. A creation of new registry keys can lead to a potential low level privilege escalation in the form of defense bypass commonly known as User Account Control (UAC) Bypass.

The scope of this product requires two components of the technician running the script. The first component is that the technician will need to have a base knowledge in the inner workings of the Windows Registry. The second component is that the technician will need to have a basic understanding in reading and modifying python scripts, specifically modifying two locations: key\_path and reg\_access. The two variables mentioned refers to the registry key location to be queried, and the root registry hive key to start with respectively. If both required components are satisfied, the technician will be able to successfully display a list of key names from the specified key location.

Github Link: https://github.com/dekripta/CYB333