**CSE 2431 Team Project**

Jacob Grove

Henry Karagory

Ian Yang

**Objective:**

Our goal is to create a kind of “malware scanner”. The user will have the ability to trigger a scan of currently running processes to search for a “bad” process. These processes will be identified if they contain any of a series of arbitrary tokens either predetermined or identified by the user. The program will automatically attempt to kill and purge any process identified by the search protocol. This will only be performed if the process can be killed safely, Additionally, the program will support a few other features. The scanner will be able to search through files that are formatted to execute instructions on Linux, and quarantine them if they meet the above criteria. Additionally, the user will be able to schedule automatic searches.

**Progress:**

So far, we have created a program entirely in the user space that can loop through files and process and identify those that meet a particular regular expression. We have enabled the ability to specify where the search criteria come from and how they are created. We have a template for implementing certain features in kernel space, including but not limited to, scheduling execution calls, hiding and unhiding files related to the search criteria per user, and a ‘safe mode’ where new created processes are checked against search criteria.

**Goals:**

We not only need to finish implementing our kernel features but bring them together in a cohesive module to append to the Linux kernel. We are still trying to identify to some extent how the work should be split among the Linux kernel and the user space. Additionally, we are trying to design a program package to be able to easily inject test examples into the OS.