Jacob Xu zx904 Assignment 2.3

This assignment has been a truly fascinating experience. While working on Task 2.2, I was astonished by the sophistication in some of my classmates' reference monitors, particularly their implementation of advanced security methods such as changing file suffixes and utilizing A/B file systems.

Interestingly, the example hint that provided test cases for attack files leveraging multi-threading was less extensive than I anticipated. Consequently, despite the greater safety afforded by using locks – since an unsafe call in R2Py is more likely to trigger an alert with lock implementation – I chose not to employ a lock-based solution.

Additionally, I identified and rectified an issue wherein a writeat operation at an incorrect offset failed to yield an EOF (End Of File) error. To address this, I introduced a new condition to validate the writeat operation by comparing the offset with the length of the file's content.

The sheer number of both invalid attacks and ineffective reference monitors surpassed my initial expectations. Although setting up the environment posed some challenges, I managed to resolve these issues successfully. In developing my attack cases, I started with a basic example attack and made slight modifications. Surprisingly, this approach alone revealed significant shortcomings in many reference monitors.

Most challenging, however, was debugging a race condition in a multi-threaded test case. The variability in logging each time made it particularly difficult to pinpoint and demonstrate the flaws in the system.

Overall, this assignment not only tested my technical abilities but also improved my understanding of system security and error handling in a dynamic, real-world context.