YAHOS – Team Contract

Members:

Guillermo Rached (rachedge@mail.uc.edu) - Developer

Thomas McCoy (mccoyt5@mail.uc.edu) - Developer

Faculty Advisor: Dr. Giovani Abuaitah

Weekly Schedule

Meetings every Tuesday and Thursday starting 3:30

Project Description

Process monitoring tool for network-based signatures and host-based signatures. Mainly targeting Windows systems, x86 architecture, with limited Linux support.

Yet Another HOst Sentinel (YAHOS) monitors running processes and their open ports for network activity. Apart from this, YAHOS can flag directories via a provided path for focused monitoring and analysis of the directory's content.

Technical details of YAHOS involve attaching to an existing process, analyzing its virtual memory, capturing network activity (if an open port is detected), and displaying real-time data. Furthermore, YAHOS can be used independently of processes to monitor directories or specific files, via interval checks, checksum validation, and other analysis techniques.

Signatures

Team Member 1: _____

Team Member 2: _____

Faculty Advisor: _____