Capstone Assessment

Guillermo Rached

As my senior design project, I chose to develop a process monitoring tool for both network-based and host-based signatures. The application, named Yet Another HOst Sentinel (YAHOS), is primarily designed for Windows systems running on x86 architecture, though it offers limited support for Linux environments. YAHOS will continuously monitor running processes and their open ports to log any network activity. In addition, the tool will allow users to flag specific directories by providing a path for detailed monitoring and analysis of the directory's contents. Some of the techniques employed by YAHOS include virtual memory analysis, packet capture, and checksum validation. The goal of this tool is to enhance system security by offering monitoring and analysis capabilities.

Throughout my academic career, I had the opportunity to take several key courses that laid the foundation for my technical knowledge. One of these was Introduction to Computer Systems (CS 2011), where I learned about essential hardware components, including registers, memory, microprocessors, and I/O ports. Additionally, I took Operating Systems and System Programming (EECE 4029), which introduced important concepts such as synchronization, inter-process communication, and networking. These two courses provided a strong foundation in lower-level computing concepts, giving me a deeper understanding of the inner workings of computer systems. This knowledge is imperative for the project, as it requires an understanding of both hardware and software at a fundamental level. The skills and insights I gained from these courses will be crucial for developing a robust and effective process monitoring tool.

In terms of professional experience, I was fortunate enough to first obtain a software engineer position with a company called Kinetic-Vision. This two-rotation experience focused mainly on full-stack web development and introduced virtualization technology. Subsequently, I secured an undergraduate research position with the University of Cincinnati through a program called RHEST, where I was exposed to academic research and current trends in cybersecurity. This exposure sparked my interest in cutting-edge cybersecurity challenges and solidified my understanding of theoretical and practical security concepts. Lastly, I worked as a cybersecurity software engineer for Northrop Grumman. This position provided me with the most insight into the cybersecurity field and greatly expanded my low-level and high-level programming skills. The combination of technical and academic skills will allow me to perform research on the problems of the state of the art and apply improvements of current methods. I expect to leverage my assembly knowledge and file structure knowledge to design the process for analysis. Overall, these

combined experiences will allow me to approach the project with a solid technical foundation and the ability to innovate on current methods.

My motivation for this project stems from my desire to contribute to the reverse engineering and cybersecurity communities by creating an open-source tool that can help others in analyzing and securing systems. I have always been fascinated by the intricate details of how computer systems operate at a low level, and this project provides the perfect opportunity to deepen my understanding while simultaneously giving back to a field that I am passionate about. Additionally, I am excited to further develop my programming skills, particularly in areas like memory analysis, network traffic monitoring, and process management. The chance to work on a project that has real-world applicability and could be useful to other security professionals drives me to ensure that the tool is both functional and impactful.

For the preliminary approach to designing the solution, I plan to start by researching existing process monitoring tools and their limitations, particularly those related to network and host-based signatures. The development will involve implementing features such as virtual memory analysis, packet capture, and checksum validation, ensuring these components work together seamlessly to provide thorough monitoring of running processes and network activity. I expect the final tool to accurately track processes, log activity, and assist in reverse engineering malware. To evaluate my contributions, I will test the tool in a virtual lab with simulated threats, verifying its accuracy and utility. Success will be measured by its ability to provide meaningful insights into system behavior, particularly when analyzing malicious software in real-world scenarios.