CSE 439 Computer Security

Term Project

A Basic Host IDS

In this project you need to design a basic IDS which will recognize any modification in a file. We assume that the files can be modified by an attacker. The file can be a binary or text file. The application that you will design will have two basic tasks.

Part I – Scanning and storing data about the files

This is essential for checkpointing the initial state of the files. You either scan the whole disk or ask user to provide a folder name for scanning. The filetypes that you are going to scan will system dependent. For windows you can scan .exe, .config and .sys file for example. When you start scanning you need to get a list of all matching files and create your data structure. The method will be designed by you. The data structure that you have created will be used in Part II.

Part II- Detecting a modification
After completing first part, your application can be run anytime. When the user wants to detect modified files, your application will go through all the files in your data structure and check if any of them has been modified. The application will list all the modified files.

Phase I: Create a design document and explain the methods you will use for your IDS. Show your data structures and the methods you will use for Part I and Part II. Due: November 20th 2019

Phase II: Implement your design. You will need to make a demo at December 4th 2019.

You should upload your design document online.

Good Luck!