Name: Syanne Voxland, Ian Jahnig, Lisa Johnson, Yasin Hussein

Proposed Topic: Topic 4: File System Analysis-Based Attack Detector

Describe the outcomes of the proposed work:

Being able to develop a software that identifies one or a few related types of attacks based on file system analysis.

What is the research question (or 2-3 closely related questions) that you intend to answer?

1. Can combining signature-based and anomaly-based detection methods improve how well we detect network attacks?
2. Does the hybrid system reduce false alarms compared to using just one detection method?

What will you need to do to answer this question (i.e., collect data, perform experiment, etc.)?  
  
Collect Data will most likely be needed to use network traffic data that includes both normal activity and attacks (e.g., from a public dataset or custom-generated traffic).

Build the System that allows a creation of the hybrid intrusion detection system that uses both signature-based detection (for known attacks) and anomaly-based detection (for unusual behavior).

Test the System that we created and run the system on test data to see how well it detects attacks.

Evaluate Results and see if what we created checks how many attacks the system catches and how many false alarms it gives, then compare it with using just signature-based or anomaly-based detection alone. If it does not work, we could possibly adjust the work or admit that we could not come up with hybrid system.