**Questions**

A Cost-Sensitive Model for Preemptive Intrusion Response Systems:

This system allows for preemptive responses to detected possible intrusions. It also allows for us to set thresholds for possible intrusions so that depending on our system’s needs, we can deploy actions more or less readily. Do we think that this is a suitable method of adaptability? On top of that, do we think the cost model for response and damage is accurate in this article? Should their be different weights assigned to each?

Model-based Response Planning Strategies for Autonomic Intrusion Protection:

We notice that this strategy for autonomic intrusion protection makes use of Markarov Decision Processes in modeling the states, actions, probabilities, and rewards. What are some of the advantages of using a Markarov Decision process when compared to some of the other methods of determining the responses to an intrusion and modeling a system’s architectural composition?

Snort: Lightweight intrusion detection for networks:

We can see that this tool can be used for real-time, lightweight intrusion detection. We also have the ability to add new rules to account for new intrusion signatures along with the signatures that we already know. How can we use this piece of technology in conjunction with another piece of software to create a comprehensive intrusion response system? We could possibly use one of the tools that we have read about this year to do so. Do we think this would be a successful intrusion response system, or would we prefer something less modular to satisfy this need?