Questions:

Performance comparison of intrusion detection systems and application of machine learning to Snort system:

This paper talks some about machine learning algorithms and applies these algorithms to intrusion detection integrated with Snort. This improves the detection rate and especially the false positive and false negative rate. What if we applied similar machine learning techniques to the response of an intrusion detection system? We've talked some about this, but I don't think we have observed the performance difference between the different machine learning techniques as they would apply to actual responses to these detected intrusions. What do we think will be the best algorithm to predict a response? What factors will it most-likely consider?

Integration of network intrusion detection systems and honeypot networks for cloud security:

This article talks about using a Honeypot to update rules for an intrusion detection system. What other pieces of information can be collected by this honey pot that would improve the intrusion detection system? What are some other factors we have discussed in class? Are there more?