Capstone Proposal

Complete or Obsolete: A re-evaluation of research

Joseph Eppich
Eppichj@sunypoly.edu

Advisor: Joshua White

State University of New York Polytechnic Institute, Utica NY
Bachelors of Science in Network and Computer Security

1   Objective:

The objective of this capstone is to read the paper "Quantitative Analysis of Intrusion Detection Systems:Snort and Suricata" and attempt at least one test present in the paper to see if the research is still valid today.

2   Rationale:

This project is important to me because I believe it is important to always re-evaluate research. With how quickly technology changes research that may have been valid in 2011 may not longer be valid with today's technology. The paper i have chosen is about the intrusion detection systems of Suricata and Snort, i hope to get a better understanding of how they work though this capstone and use that knowledge in the near future.

3   Approach:

I plan on approaching this capstone through several steps. First I will conduct research on the paper I have chosen, I will do this by reading the paper and taking notes. Second I plan on taking at least one of the tests used in the paper and preforming it myself recording my results. Lastly I will compare my results with the intials results and record my findings.

4   Timeline:

Give a bulleted timeline of when you will have things completed. Don't forget to include the Student Undergraduate Research Expo poster presentations, and final presentation in your timeline.

You can create bullets by doing:

- (2/25)have a basic idea and outline for my paper
- (3/1) have my capstone proposal made and submitted, and begin researching
- (4/19) have my paper finished submitted for final review
- (5/1) proof read and look over all my material and prepare for my presentation

5   Possible Issues:

Possible problems I foresee with this capstone is my lack of hardware compared to that used in the original content. beyond that technical issues with suricata and snort could lead to issues in the long run.