# [Intrusion Detection Analysis on Vulnerable Docker Container]


**Key Contributors:**

**David Grant, Gabriel Ream, Joseph Drouillard**



**10-21-2022**

This project and the preparation of this report were funded in part by ….through an agreement with the University of the Incarnate Word.
Cyber Security Systems and the University of the Incarnate Word

# EXECUTIVE SUMMARY

This project is meant to be an implementation and demonstration of an IDS system. Our project involves capturing and visualizing the data collected by a host IDS on a vulnerable Docker container which is under attack by another container. This data is captured, parsed, and filtered onto Elasticsearch for visualization and analysis using Kibana. Our report is meant to be a demonstration of the effectiveness of our IDS.

Project Milestones:

1. Create an “attack” and a vulnerable container on Docker
2. Implement a functional host-based IDS on the vulnerable container
3. Connect the IDS to Elasticsearch
4. Execute attacks on the vulnerable container
5. Collect IDS data
6. Structure, visualize, and analyze the IDS data in Elasticsearch
7. Create a final report analyzing our findings
8. Create a final PowerPoint presentation

Materials List:

1. “Attacker” Ubuntu container on Docker
2. Vulnerable container on Docker from Vulnhub
3. Preexisting Github code for use in the IDS implementation
4. IDS system
5. Elasticsearch and its tools (including Kibana)

Deliverables:

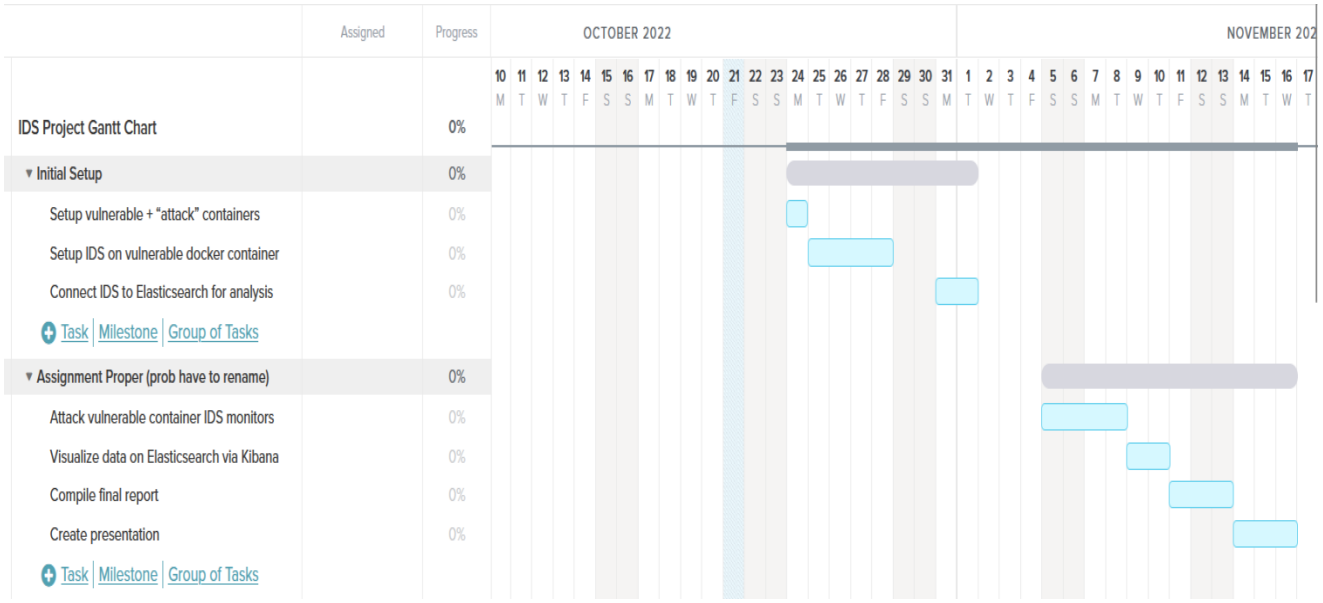
1. A vulnerable and “attacker” Docker container
2. A functioning IDS system on the vulnerable container
3. Visualization of the IDS data through Elasticsearch Kibana
4. Final formal report on findings
5. Final slide presentation on findings

Professional Accomplishments:

1. Additional experience attacking other systems
2. Knowledge in configuring and deploying a host-based IDS
3. New skills in piping and visualizing IDS data through Elasticsearch

# PROJECT SCHEDULE MANAGEMENT

**Our Gantt Chart schedule:**




Create a Github Project Repository and add the user "cyberknowledge" as a contributor:

gabeream/Intrusion-Detection-Analysis-on-Vulnerable-Container (github.com)

Intrusion Detection Analysis on Vulnerable Container | Trello