Jonathan Ho

jlh5360@rit.edu

Team Bravo

CSEC 473.02

2235 Spring

HW3 Gray/Purple Teaming

CCDC Rule: "Use of public forums (blog posts, stack overflow) is encouraged. Sites which require a subscription to access info are not permitted"

Aspect: Docker/Docker Compose for hosting a scoring engine/score checker for a cyber security Red/Gray/Blue team competition

Metrics: Response time and scalability

1. **For your selected rule for your competition:**
    a. **Explain what it's purpose is?**

    The purpose of encouraging the use of public forums such as blog posts and Stack Overflow, while prohibiting sites requiring a subscription, is to facilitate knowledge sharing and collaboration among participants without any paid services that would or will allow them to cheat. By allowing access to freely available resources, participants can enhance their problem-solving skills and learn from the collective expertise of the cybersecurity community.

    b. Why it is necessary for a successful competition?

    This rule is necessary or an essential for a successful (Red/Gray/Blue team cyber security) competition as it promotes a fair and even level playing field and environment where all participants are authorized to have access to the same resources. Moreover, by encouraging the use of public forums, it ensures that participants can leverage external knowledge to address challenges encountered during the competition. As a result, encouraging or promoting a culture and environment of continuous learning and skill development with deep motivation.

    c. How it will be enforced?

    The enforcement of this rule will be communicated clearly to all participants through competition guidelines and briefings. Monitoring mechanisms and

services to view each computer's screen may be employed to allow us, Gray team, to monitor their actions. In addition, this monitoring mechanism may be implemented in a say to detect people trying to request access to prohibited sites requiring a subscription. With that being said, any and all participants who are discovered violating this rule may receive penalties like losing points and or disqualification, emphasizing the importance of adhering to competition rules.

2. **For your selected "aspect" to be assessed for your competition:**
   a. **Why is this "aspect" important to your competition?**

The scoring engine or score checker is important in the cybersecurity competition as it evaluates the performance of participants of both teams (Blue and Red teams, mainly the two Blue teams), assessing the effectiveness of defensive measures, and quantifying the impact of simulated attacks by evaluating it in the concept of points. Therefore, it serves as a critical tool for both red and blue teams, providing objective metrics for performance evaluation and feedback.

   b. **How will this "aspect" be sampled/observed/measured?**

The aspect of Docker/Docker Compose being used or hosting scoring engine service will be assessed through various criteria, including: system performance, reliability, scalability, and accuracy of scoring. Observations will be made before the competition to perform necessary tests and adjustments, and during the competition to evaluate how well the scoring engine functions in real-world scenarios and its ability to handle many concurrent user interactions and workload. Furthermore, key metrics such as system uptime, responsiveness, accuracy of scoring, and scalability will be implemented and evaluated to measure or determine the effectiveness of the scoring engine in accurately assessing participant actions and responses.

   c. **What is the metric used?**

The metric used to assess the scoring engine's performance may include but not limited to are:

- Response Time: This metric measures the speed at which the scoring engine processes and responds to participant interactions and updates; so, a lower response time indicates better performance and efficiency, ensuring timely feedback to participants.
- Scalability: This refers to the ability of the scoring engine to handle and accommodate the increasing loads and multiple concurrent user interactions without experiencing a decrease in performance. It ensures that the scoring engine will remain effective and efficient even as accommodate a growing number of participants and tasks.