Concordia Institute for Information Systems Engineering (CIISE)

Concordia University

INSE 6130 OPERATING SYSTEM SECURITY

Project Proposal:

IMPLEMENTING RECENT ATTACKS AND A SECURITY APPLICATION ON CONTAINER

Submitted to:
Professor SURYADIPTA MAJUMDAR

Submitted by:

Student Name	**Student ID**	**Role**
Jubin Raj Nirmal	40235087	Attack
Oladeinde Sukurat	40181568	Attack
Musthafa Talha Ucar	40059335	Defense
Eyiba Precious	40157231	Defense
Sanchit Smarak Behera	40230269	Defense
Anita Francis Archibong	27729790	Attack
Hulli Rahul Ravi	40234542	Defense
Patel Riya Vinodbhai	40224858	Attack

Project Overview:

To implement a set of recent attacks on a container system and use defense mechanisms to counter them.

Team Members:

We are a group of eight (8) members. Four members will contribute to the attack phase of the project and rest will contribute to the defense phase (Security Application). The names of the members, their student IDs and roles are stated as below.

Project Description:

The project will be divided into three parts.

1: The Attack Phase: Here, we would use 5 different attacks, one of which would be a computer virus. The target system will be a docker container. The operating system used for the attack would be Kali Linux.

Each attack would be done via a Kali Linux system, which would exploit the network end vulnerabilities and penetrate the container system and pass the payload. The virus will be injected via a USB drive.

2: Data collection and Research: Here, we would use tools to gather information of the state of the system before, during and after the attack. All of these will be documented, which will help us for the defense phase.

The tools that would be used to gather information is not yet decided, but the information that will be gathered would be as follows:

- Folder structure changes before and after the payload action.
- CPU usage changes before and after the payload action.
- Ports exploited.
- Type of attack and type of damage.

The anatomy of the virus used would also be studied and the attacking subroutine would be recognized and categorized. This will be added to the research.

3: Defense Phase: The data acquired during research will be used in the defense phase to decide a security measure to counter the attack. This defense software would be coded and used against the attacks and tested for its effectiveness.

The defense method would be decided based on which defense idea or strategy would work best against all of the attacks, and at the same time, does not take a load on the CPU.

Purpose and background:

The Attack-and-Defense strategy (or the Red team, Blue team strategy) is a common method to detect vulnerabilities in any type of environment – Operating Systems to even native applications. The red team (attacking team) attacks the environment, and the blue team (defense team) implements solutions against the attack. This is a pro-brainstorming method of bombarding all types of possible ideas via experts, in-turn making the service more layered and immune against attacks no matter how recent they get. It creates not only a competitive environment, which can be a fun experience, but also a live testing environment, where the service gets exposed to attacks not seen before.

Proposed Solution:

Our end goal is to simply come up with a defense software that mitigates all the attacks used during the attack phase.

Scope of work

The attack phase here, not only talks about the payloads in action, but also the manner of deployment. A group of four (4) attackers would decide on the manner of attack and pushing the payload onto the container system. The attacks used will be decided, tested, and deployed, bypassing all security checks. A computer virus will also be deployed, but through a USB drive and its actions will be monitored and controlled at the attacker end.

The research phase will be taken forward by all the members of the team in turns to understand the damage done by the attacks. Information will be gathered as mentioned in the project description.

The defense phase will be carried out by the other group of four (4) defenders. A defense solution would be decided based on the information gathered and a software solution would be built. The software solution may have more than one type of defense solution, and different members would be responsible to code each of it.

Conclusion:

The proposed project would be undertaken over a span of four months and detailed progress and final reports would be shared once the project is completed.