Concordia Institute for Information System 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
Devanshi Rajpara	40164374	Web-Developer
Jeevesh Awal	40169864	Application and Security Architect
Lakshay Bareja	40156832	Host Attacking and Linux Developer
Meghrajsinh Chauhan	40156699	Application Attacking and Host Security
Nithish Reddy Yalaka	40164619	UI Architect and Scrum Master
Rohan Pagey	40168378	Attack Strategy and Implementation
Venkata Narsu Pavani Shrinija Dosapati	40162308	UI Designer
Siva Teja Narayanabhatla	40166568	UI Designer

Technology Stack

- Container = Docker
- Container Image = Ubuntu
- Application Backend = PHP
- Application Database = MySQL
- Attacking VM = Kali Linux
- Host for Docker = Linux

Overview

We would gain access to the system via a web application running on a Docker Container by finding vulnerabilities and exploiting them to find our way to the host system. We would start by creating a containerized web environment with some known vulnerabilities and run-time Docker misconfigurations. By exploiting the web application, we would gain access to the docker container using command injection, allowing us to access the host system using container break-out techniques. We would be preventing the attack on the application layer from restricting the attacker's entry into the container environment and thus the host system. Along with implementing web application-level security, we would also be deploying custom services inside the Container, which would handle the privilege escalation attacks.