

Concordia Institute for Information Systems Engineering (CIISE)

Concordia University

**INSE 6130 Operating System Security Project Proposal**

Submitted to:

**Professor Dr. Suryadipta Majumdar**

Submitted By:

|  |  |  |
| --- | --- | --- |
| **Student Name** | **Student ID** | **Role** |
| Avin Vincent | 40265132 | Attack Implementation |
| Likitha T Reddy | 40265131 | Attack Implementation |
| Challa Likitha | 40293973 | Attack Implementation |
| Chinnabathini Hima Bindu | 40292127 | Attack Implementation |
| Moksh Sood | 40294266 | Attack Implementation |
| Yash Khosla | 40232363 | Security Implementation |
| Kunati Bala Krishna Yadav | 40292128 | Attack and Security Implementation |
| Divya Varshini Murathoti | 40293222 | Security Implementation |

**Project Overview**

To gain practical experience with the real-world security breaches and enhance our hands-on skills, thereby immersing ourselves in the realm of container technology. By implementing defensive strategies within this widely-used technology, we can deepen our understanding of security threats and refine our ability to mitigate them effectively.

**Team Members**

We are a group of eight members. Among these, five members will contribute to the attack phase and the rest will contribute to the defence phase as stated above.

**Project Description**

Docker platform has faced various security challenges across different operating systems. Most attacks often exploit vulnerabilities in Docker's architecture and configurations in order to gain privilege escalation. As part of the project's attacks on Docker, we will be demonstrating several attacks encountered in Desktop & UNIX versions. Attacks would be carried out mostly using Virtual Machines and may vary depending on the attack.

We will be noticing the levels of easiness for deploying the payloads and most attacks would be focusing on performing privilege escalation in order to access or execute restricted binaries. The attacks might be categorized based on the Common Vulnerabilities and Exposures [CVE] identifiers or the way vulnerabilities are attributed such as file-descriptor mishandling, broken access control, through malware or even misusing the existing administrative privileges of diagnostics collection.

Upon successfully demonstrating the exploitation of vulnerabilities, our aim is to provide comprehensive recommendations for preventing such breaches. As part of concluding this project, we will practically implement essential security measures, including APPARMOR profiles and SECCOMP Security Policies. By incorporating these security measures, we fortify Docker against the aforementioned attacks ensuring a more secure environment for containerized applications. Additionally, we will explore other best practices and strategies to further enhance Docker’s security posture and protect against emerging threats.

**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.