INSE 6130 Operating System Security

Project Requirements

Notice:

- This is a group project. The size of the group must be between 7 and 8 (no exception). It is your responsibility to organize, and work as, a team. You should anticipate and learn to deal with potential conflicts. It will help to clearly state each member's responsibility as early as possible (such as in proposal) and then stick to it. Also, you may divide tasks such that each member's job is less dependent on others' outcome.
- In most cases, grade is given to a group, not individual. If there's plagiarism in the group's report, then everyone will be responsible. I will do my best to identify any plagiarism in your report, and will have zero tolerance regarding this. Here plagiarism is defined as the copy-and-paste of a complete sentence or anything more significant.

Overview:

The objective of this project is twofold: to expose you to real world security attacks and improve your hands-on skills through implementing defense mechanisms in one of the most popular technologies – container[1]. The project will include two parts, each of which counts for 50% mark of the project:

1. Implementing recent attacks on container.
2. Implementing a security application on container.

Interaction between those two parts of the project (e.g., showing how the security application can catch or prevent one of the implemented attacks) would be a bonus, but not required.

Project Details:

Each group should implement a couple of recently seen attacks on container platforms. The attacks must be exploiting vulnerabilities in the platform itself (so you cannot install an application on the platform and then attack that application). Each group should also implement one security application (e.g., permission management or access control, authentication, intrusion detection, privacy protection, etc.) for containers. The two implementations could be independent, or related (which will be a bonus).

The implementation of both attacks and security application should be based on virtual environment, and isolated from the network (be very careful and remember you will be solely responsible if anything goes wrong). It is up to you to decide how many/which attacks, and what kind of security application to implement. The onus is on you to demonstrate to me that your team has done enough and quality work through the final report and presentation/demo. The final report must be submitted together with the source code of the

[1] What is container: https://www.docker.com/resources/what-container

security application. It must also provide enough details about launching the attacks and running the security application such that I can duplicate and verify your implementations.

Deliverables:

1. Proposal: Each group should submit a proposal before the deadline (see class webpage). The proposal must clearly state the following.

- The team members' names.
- Who is going to do what (especially, who will implement the attacks and who will implement the security application).

(There is no need to decide exactly which attacks or app to implement in the proposal.)

2. Presentation: Each group must prepare a pre-recorded, around 10-minute long video, to be submitted by each group through the EAS before the deadline (see class webpage). The video should start with 3-5 PowerPoint slides to introduce your project, followed by a short demo of both the attacks and security app your group has implemented. The video should include either audio or subtitles to explain each slide and the demo.

3. Reports: Each group should submit a progress report (7-10 pages) and a final report (15-20 pages excluding appendix) before the respective deadlines. The final report must show clear evidences about the quality and quantity of work (e.g., detailed descriptions of the implementation, screen shots of the attacks and application, encountered challenges and solutions, etc.). The goal is to convince me that you have done a lot and learned a lot from the project. The report should use font size 11, single line space, and reasonable margins. The reports should clearly describe each member's contribution.