INSE 6620 Cloud Computing Security and Privacy

Project Requirements

Notice:

- This is a group project. The size of a group must be 6-7 (no group smaller than 6 will be allowed due to the class size). It is your responsibility to organize, and work as, a team via regular meetings, email exchanges, etc. 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-pasted, or AI (e.g., ChatGPT)-generated, content of a complete sentence or anything more significant.

Overview:

The objective of this project is to expose you to real world cloud platforms and improve both your hands-on skills and the capability of presenting the results.

This project will include *two* parts, each of which counts for 50% mark of the project:

1. Install OpenStack on your own computer and use it to deploy a small virtual network (with >= 2 nodes).
2. Using this virtual network, launch a network-based attack and detect it with Snort.

Project Details:

1. Install OpenStack and deploy a virtual network (50% marks):

Each group should install OpenStack on a local computer, and use it to set up a small virtual network with at least 2 nodes.

Keep track of all the details/challenges/failures/solutions as you work on this, since all of those will be expected in your final report.

2. Launch and detect a network-based attack (50% marks):

The only requirement for the attack is that it must be network-based, i.e., it must be launched from one node and target another node of your virtual network. You can use any existing exploit code.

Important: Be very careful playing with real world attacks, and you'll be responsible for any consequences if your attack gets out of control.

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.
- Task distribution (who is going to do what).
- Specifications of the machine you plan to use, which should meet the requirements of installing and working with OpenStack.

2. Presentation: The project presentation should be a 10-minute long, pre-recorded video, to be submitted together with the final report by each group through the EAS before the deadline (see class webpage). The video should start with 3-5 PowerPoint slides to briefly introduce your project, followed by a short demo of the functional virtual network, the attack, and its detection with Snort. The video should include either audio or subtitles to explain each slide and the demo. The presentation is to be submitted via EAS before the deadline (see class webpage).

3. Final report: Each group should submit a final report (around 10 pages, excluding references/ appendices). The report should use font size 11, single line space, and reasonable margins. The report should provide all the technical details (e.g., through screenshots), especially the challenges encountered and your solutions. The point is to convince me that you have tried something challenging (to you) and learned a lot from it. The report should clearly describe each member's contribution. The report is to be submitted via EAS before the deadline (see class webpage).