Previous Sprint goals

- Create basic environment for running containers
- Fill the containers with potentially old or vulnerable software
- Try to use popular tools to define vulnerabilities
- Have script that can access the code and containers

Achievement

- **Create basic environment for running containers**
  - Run docker containers on local machines
- **Fill the containers with potentially old or vulnerable software**
  - Filled the containers with potentially vulnerable and also secure containers
  - Managed to execute some vulnerability and get inside or at least breach
- **Try to use popular tools to define vulnerabilities**
  - Used Snyk to check the containers

What did not work?

- **Environment**
  - SSC does not support container virtualization (security issues)
- **Fill the containers with potentially old or vulnerable software**
  - It is difficult to check running container because files are used
  - Looking for ways to get access to files in container and image
- **Try to use popular tools to define vulnerabilities**
  - There is to many vulnerabilities even in official containers

Next Sprint goals

- Find the way to access the data in image and container if possible
- Try to get the running version of software
- Try to check opened ports
- Try to make your own layered image
- Logging what happens
- Check what user is running container block root
- Check for privileged mode
- Scan for Secrets
- Restricting what container can do in core system
- Intercontainer communication