Question 1 of 7

Which seccomp profile does Kubernetes use by default?

- ○ Secure
- ○ Default
- ● None – seccomp is not enabled by default

Question 2 of 7

How should you decide which syscalls to block?

- ○ Block all of them, just to be sure
- ● Figure out which syscalls you need and block the rest
- ○ Block syscalls relating to file manipulation

Question 3 of 7

Which action can be used to allow syscalls?

SCMP_ACT_ALLOW

Question 5 of 7

Which seccomp profile object type should be used for a custom seccomp profile on the host?

Localhost

Question 5 of 7

Which seccomp profile object type should be used for a custom seccomp profile on the host?

Localhost

Question 6 of 7

What is the token for modifying and applying the correct seccomp profile?

7cee0b The Token might be different, change it to the one in your terminal output

---

Question 6 Steps:

- Use vi editor to update seccomp-profile.json, remove keyctl from the names section.

- Use vi editor to update manifest.yaml, completed content shown as below

Kubernetes

```
apiVersion: v1
kind: Pod
metadata:
  name: emma-pod
  labels:
    app: emma-pod
spec:
  securityContext:
    seccompProfile:
      type: Localhost
      localhostProfile: seccomp-profile.json
  containers:
  - name: test-container
    image: hashicorp/http-echo:0.2.3
~
```

- Apply the change, and you will get the token

Kubernetes

```
linux@k8s-master:~$ kubectl apply -f manifest.yaml
pod/emma-pod created
linux@k8s-master:~$
Your token for question six is 7cee0b
```

Question 7 of 7

Why should the ioperm syscall be blocked by a seccomp profile?

- ○ It is malware
- ○ It should not be blocked because it is not blocked by default
- ◉ Allowing a compromised container to modify kernel privilege can lead to the host being compromised