Free Questions for CKS by dumpssheet

Shared by Keller on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Given an existing Pod named nginx-pod running in the namespace test-system, fetch the service-account-name used and put the content in /candidate/KSC00124.txt

Create a new Role named dev-test-role in the namespace test-system, which can perform update operations, on resources of type namespaces.

Options:

A) Create a new RoleBinding named dev-test-role-binding, which binds the newly created Role to the Pod's ServiceAccount (found in the Nginx pod running in namespace test-system).

Answer:

A

Question 2

Question Type: MultipleChoice

Before Making any changes build the Dockerfile with tag base:v1

Now Analyze and edit the given Dockerfile(based on ubuntu 16:04)

Fixing two instructions present in the file, Check from Security Aspect and Reduce Size point of view.

Dockerfile:

```
FROM ubuntu:latest

RUN apt-get update -y

RUN apt install nginx -y

COPY entrypoint.sh /

RUN useradd ubuntu

ENTRYPOINT ['/entrypoint.sh']

USER ubuntu
```

entrypoint.sh

```
#!/bin/bash

echo 'Hello from CKS'
```

After fixing the Dockerfile, build the docker-image with the tag base:v2

Options:

A) To Verify:Check the size of the image before and after the build.

Answer:

A

Question 3

Question Type: **MultipleChoice**

On the Cluster worker node, enforce the prepared AppArmor profile

```
#include <tunables/global>

profile docker-nginx flags=(attach_disconnected,mediate_deleted) {

#include

network inet tcp,

network inet udp,
network inet icmp,
deny network raw,
deny network packet,
file,
umount,
deny /bin/** wl,
deny /boot/** wl,
deny /dev/** wl,
deny /etc/** wl,
deny /home/** wl,
deny /lib/** wl,
deny /lib64/** wl,
deny /media/** wl,
deny /mnt/** wl,
deny /opt/** wl,
deny /proc/** wl,
deny /root/** wl,
deny /sbin/** wl,
deny /srv/** wl,
deny /tmp/** wl,
deny /sys/** wl,
deny /usr/** wl,
audit /** w,
/var/run/nginx.pid w,
/usr/sbin/nginx ix,
deny /bin/dash mrwklx,
deny /bin/sh mrwklx,
deny /usr/bin/top mrwklx,
capability chown,
capability dac_override,
capability setuid,

capability setgid,

capability net_bind_service,

deny @{PROC}/* w, # deny write for all files directly in /proc (not in a subdir)

# deny write to files not in /proc/<number>/** or /proc/sys/**

deny @{PROC}/{[^1-9],[^1-9][^0-9],[^1-9s][^0-9y][^0-9s],[^1-9][^0-9][^0-9][^0-9]*}/** w,

deny @{PROC}/sys/[^k]** w, # deny /proc/sys except /proc/sys/k* (effectively /proc/sys/kernel)

deny @{PROC}/sys/kernel/{?,??,[^s][^h][^m]**} w, # deny everything except shm* in /proc/sys/kernel/

deny @{PROC}/sysrq-trigger rwklx,

deny @{PROC}/mem rwklx,

deny @{PROC}/kmem rwklx,

deny @{PROC}/kcore rwklx,

deny mount,

deny /sys/[^f]*/** wklx,

deny /sys/f[^s]*/** wklx,
deny /sys/fs/[^c]*/** wklx,

deny /sys/fs/c[^g]*/** wklx,

deny /sys/fs/cg[^r]*/** wklx,

deny /sys/firmware/** rwklx,

deny /sys/kernel/security/** rwklx,

}
```

Edit the prepared manifest file to include the AppArmor profile.

```
apiVersion: v1

kind: Pod

metadata:

name: apparmor-pod

spec:

containers:

- name: apparmor-pod

image: nginx
```

Finally, apply the manifests files and create the Pod specified on it.

Verify: Try to use commandping, top, sh

Options:

A) Explanation:

Answer:

A

Question 4

Question Type: MultipleChoice

A container image scanner is set up on the cluster.

Given an incomplete configuration in the directory

Options:

A) 1. Enable the admission plugin.
2. Validate the control configuration and change it to implicit deny.
Finally, test the configuration by deploying the pod having the image tag as the latest.

Answer:

A

Question 5

Question Type: **MultipleChoice**

Secrets stored in the etcd is not secure at rest, you can use the etcdctl command utility to find the secret value

for e.g:-

Options:

A) ETCDCTL_API=3 etcdctl get /registry/secrets/default/cks-secret --cacert='ca.crt' --cert='server.crt' --key='server.key'
Output

Image not found or type unknown

Using the Encryption Configuration, Create the manifest, which secures the resource secrets using the provider AES-CBC and identity, to encrypt the secret-data at rest and ensure all secrets are encrypted with the new configuration.

Answer:

A

Question 6

Question Type: **MultipleChoice**

Using the runtime detection tool Falco, Analyse the container behavior for at least 20 seconds, using filters that detect newly spawning and executing processes in a single container of Nginx.

Options:

A) store the incident file art /opt/falco-incident.txt, containing the detected incidents. one per line, in the format [timestamp],[uid],[processName]

Answer:

A

Question 7

Question Type: **MultipleChoice**

Use the kubesec docker images to scan the given YAML manifest, edit and apply the advised changes, and passed with a score of 4 points.

kubesec-test.yaml

```
apiVersion: v1

kind: Pod

metadata:

name: kubesec-demo

spec:

containers:

- name: kubesec-demo

image: gcr.io/google-samples/node-hello:1.0

securityContext:

readOnlyRootFilesystem: true
```

Options:

A) Hint:docker run -i kubesec/kubesec:512c5e0 scan /dev/stdin < kubesec-test.yaml

Answer:

A