



Free Questions for CKS by [braindumpscollection](#)

Shared by [Moon](#) on 07-06-2022

For More Free Questions and Preparation Resources

[Check the Links on Last Page](#)

Question 1

Question Type: MultipleChoice

SIMULATION

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.

store the incident file art /opt/falco-incident.txt, containing the detected incidents. one per line, in the format

[timestamp],[uid],[processName]

Options:

A) Send us the Feedback on it.

Answer:

A

Question 2

Question Type: MultipleChoice

SIMULATION

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

kubesecc-test.yaml

apiVersion: v1

kind: Pod

metadata:

name: kubesecc-demo

spec:

containers:

- name: kubesecc-demo

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

securityContext:

readOnlyRootFilesystem: true

Hint:docker run -i kubesecc/kubesecc:512c5e0 scan /dev/stdin

Options:

A) Send us the Feedback on it.

Answer:

A

Question 3

Question Type: MultipleChoice

SIMULATION

Service is running on port 389 inside the system, find the process-id of the process, and stores the names of all the open-files inside the /candidate/KH77539/files.txt, and also delete the binary.

Options:

A) Send us your feedback on it.

Answer:

A

Question 4

Question Type: MultipleChoice

SIMULATION

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:-

```
ETCDCTL_API=3 etcdctl get /registry/secrets/default/cks-secret --cacert="ca.crt" --cert="server.crt" --key="server.key"
```

Output

```
/registry/secrets/default/cks-secret
k8s
v1 secret
cks-secret "default"*$67fcb53f-6b58-4fee-9f12-5737c764be742
kubectl create update secretsV1:9
{"f:key1":{"f:type":"visible"}, "f:key2":{}}, {"f:type":{}}
key1
supersecret
key2 topsecret opaque
Visible
```

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.

Options:

A) Send us the Feedback on it.

Answer:

A

Question 5

Question Type: MultipleChoice

SIMULATION

Create a Pod name Nginx-pod inside the namespace testing, Create a service for the Nginx-pod named nginx-svc, using the ingress of your choice, run the ingress on tls, secure port.

Options:

A) Sendusyourfeedbackonit

Answer:

A

Question 6

Question Type: MultipleChoice

SIMULATION

On the Cluster worker node, enforce the prepared AppArmor profile

```
#include
```

```
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/** 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 rwkx,  
  
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/** rwkx,  
  
deny /sys/kernel/security/** rwkx,  
  
}
```

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) Send us the Feedback on it.

Answer:

A

To Get Premium Files for CKS Visit

<https://www.p2pexams.com/products/cks>

For More Free Questions Visit

<https://www.p2pexams.com/linux-foundation/pdf/cks>

