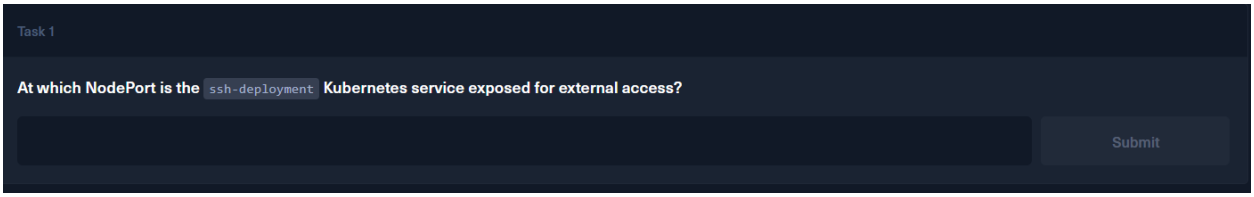
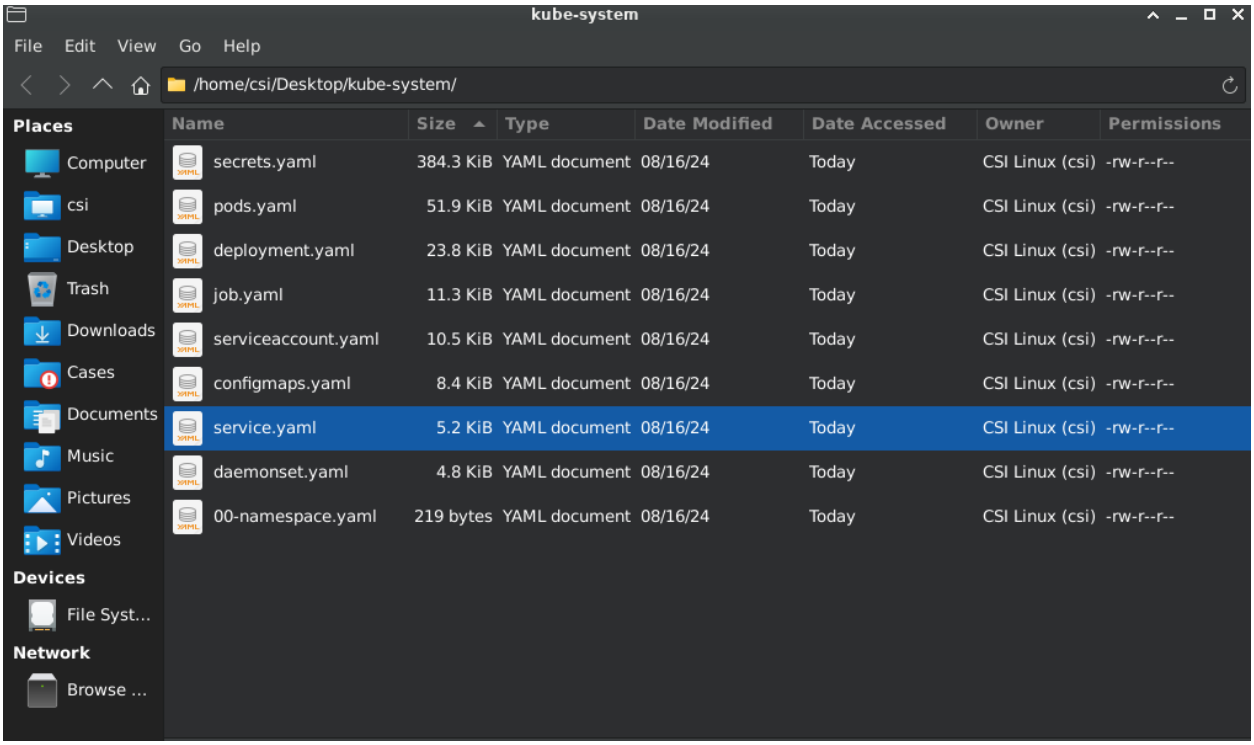
Sherlock Scenario

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.

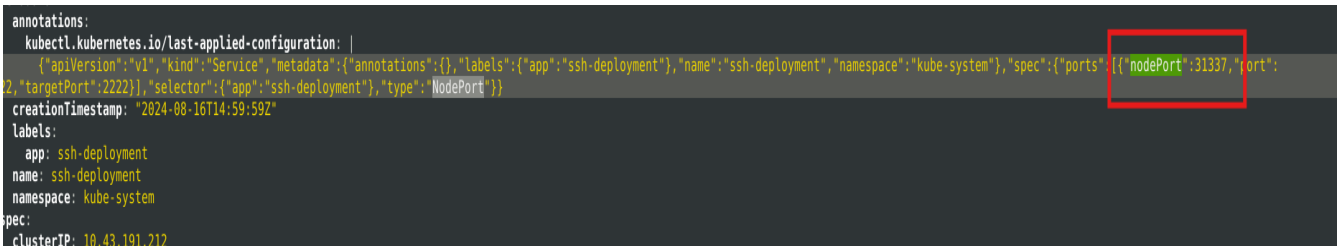
1-flag



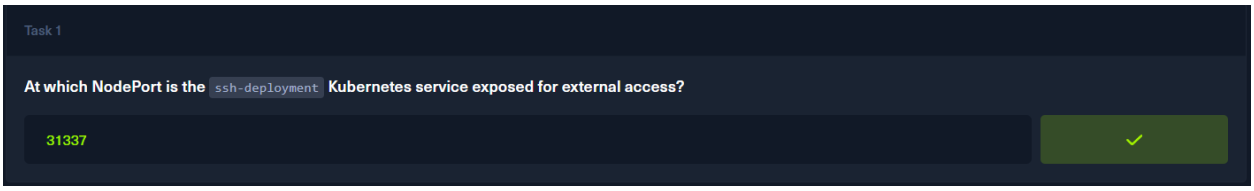
Para encontrar el nordeport nos dirigimos a los archivos proporcionados por el ctf y vamos a service.yaml



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



La flag es: 31337



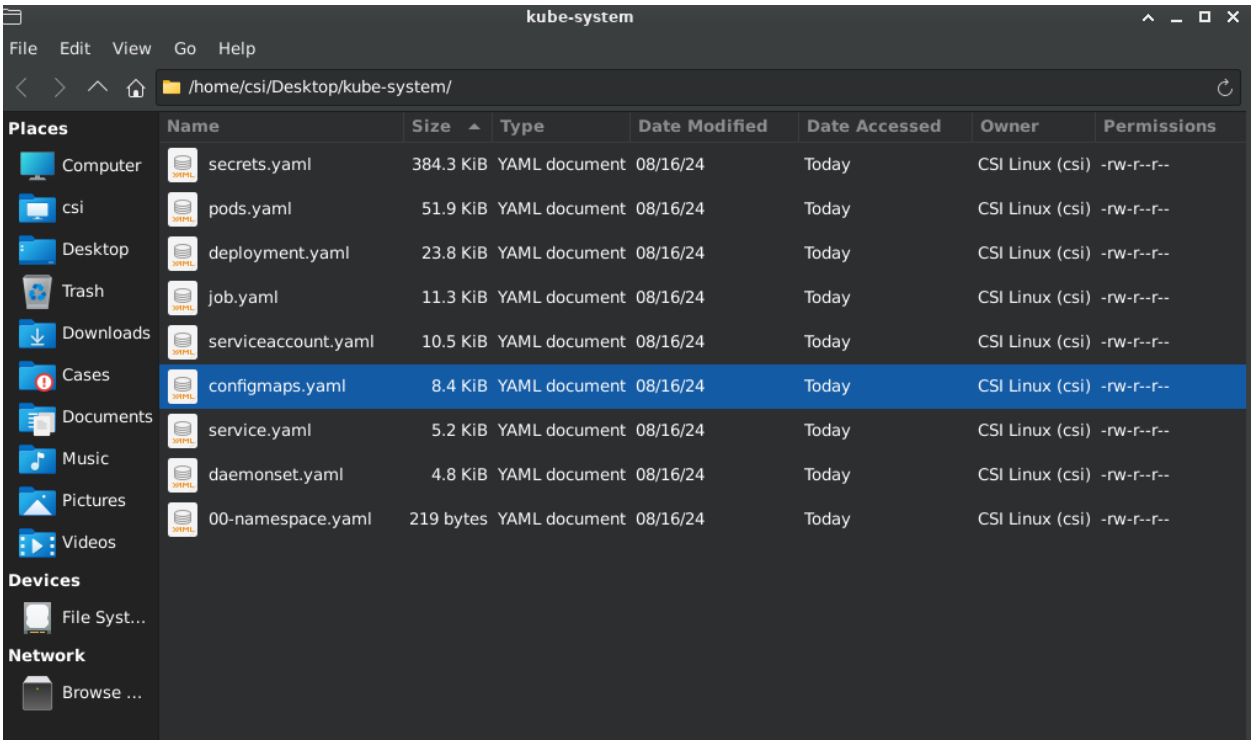
2-flag

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

La flag: **10.43.191.212**

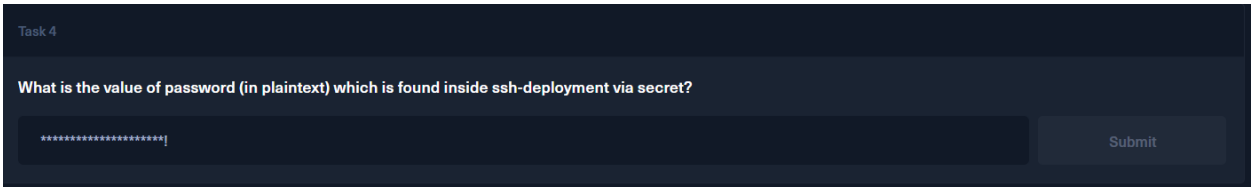
3-flag

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



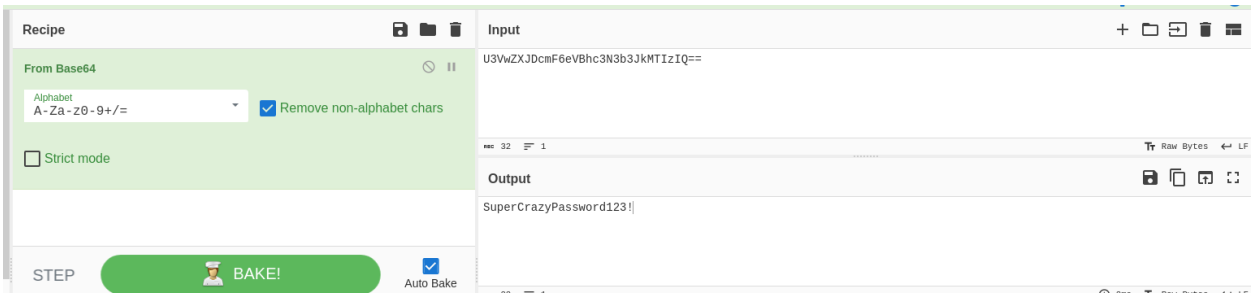
La flag es: **HTB{1d2d2b861c5f8631f841b57f327f46f8}**

4-FLAG

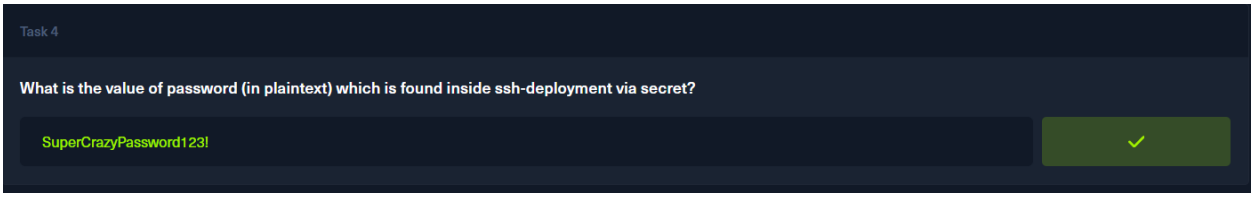


Para encontrar esta flag me dirigí a secre y filtré por password y encontre un user_password con la password cifrada en base 64

Procedi a decifrar el codigo en ciberchef el cual me dio la password

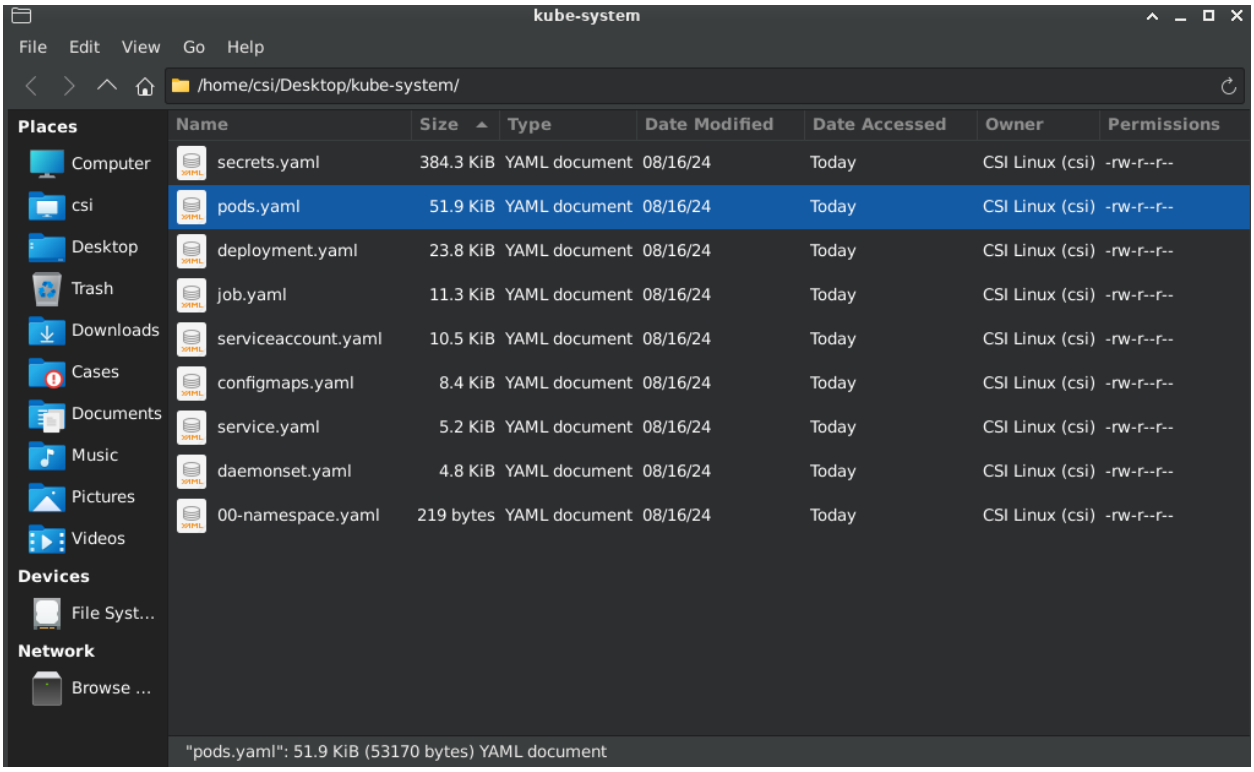


La Flag es: **SuperCrazyPassword123!**



5-Flag

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



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

6-Flag

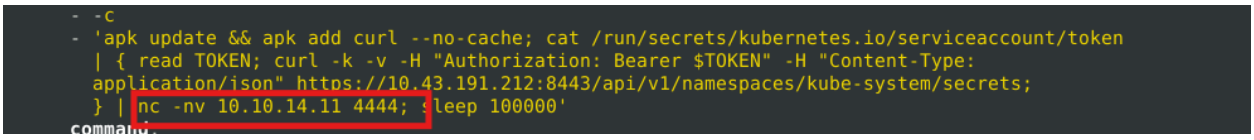
Visualizando el codigo me percate del nombre de la imagen utilizada por el atacante

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

La flag es: **alpine**

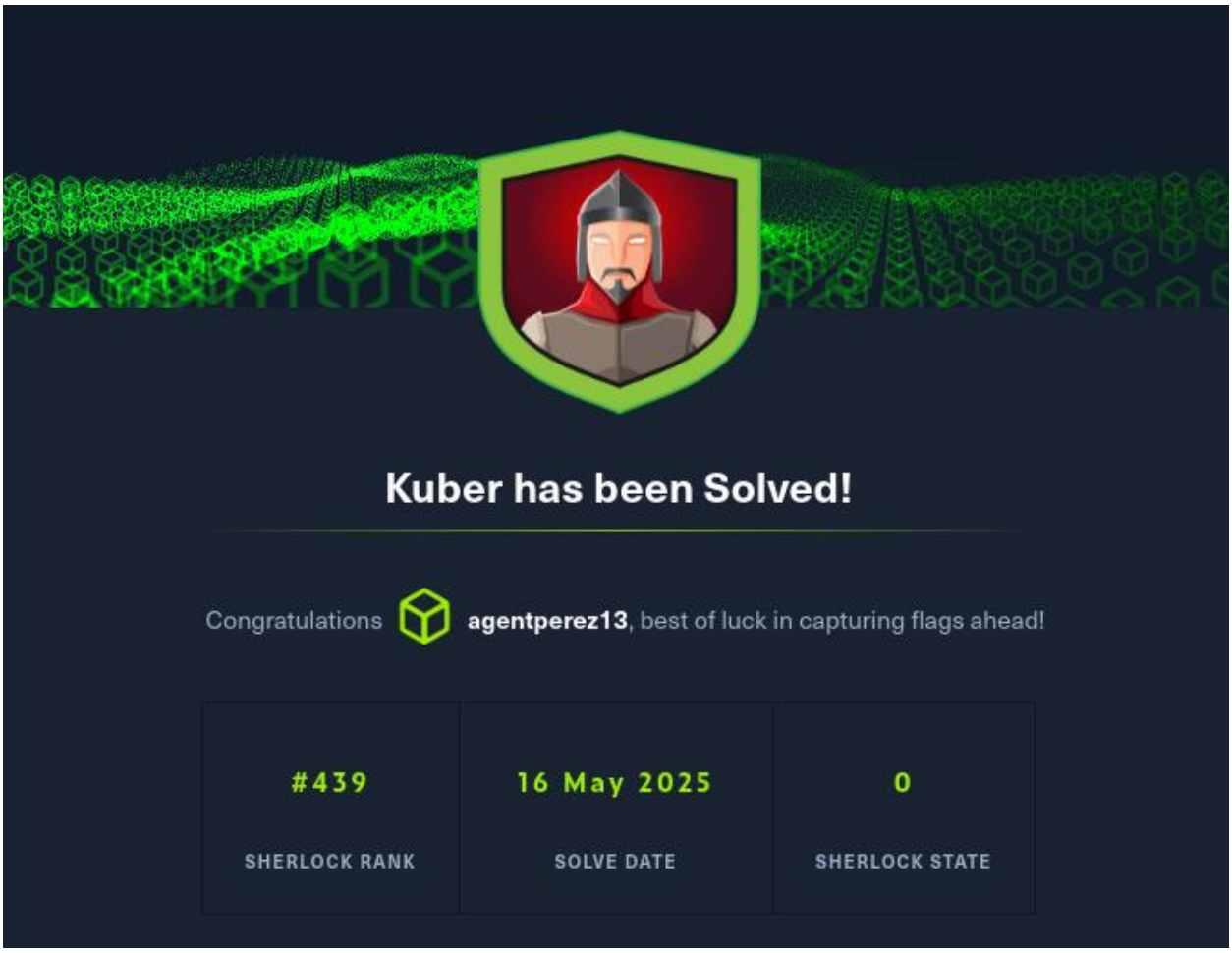
7-Flag

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



La flag: 1**0.10.14.11**


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