Kubernetes and Container Security: Hands-On Introduction

 Start Machine

Welcome to Kubernetes and Container Security: Hands-On Introduction, as presented at [The Diana Initiative](https://www.dianainitiative.org/) 2020! This material was developed for challenge #19 in the CTF, and the walkthrough was presented live on Saturday, 20202/08/22 at 1:00PM PDT.

The goal of this workshop is to help introduce you to the basic concepts of hacking Kubernetes. The intended audience is folx with offensive security or pentesting experience who want to learn about Kubernetes, or Kubernetes engineers who are beginning to think about the potential abuse of their clusters.

If you're new to Kubernetes, I highly recommend you begin by watching the beginning of [the walkthrough](https://www.youtube.com/watch?v=n-SJe2PXF_E)(up to about minute 23) to become familiar with the terms and concepts. Then, try to solve the challenge on your own; it has a lot of built-in hinting to help you progress. Of course, if you get stuck, you can always go back to the video for explicit instruction.

To begin, you'll want to boot the VM, install kubectl, and download the challenge kubeconfig file from Task #2 so you can connect to Kubernetes.

Pull up a chair, warm up your terminal, and get ready to hack my cluster! I'm so glad you're here.

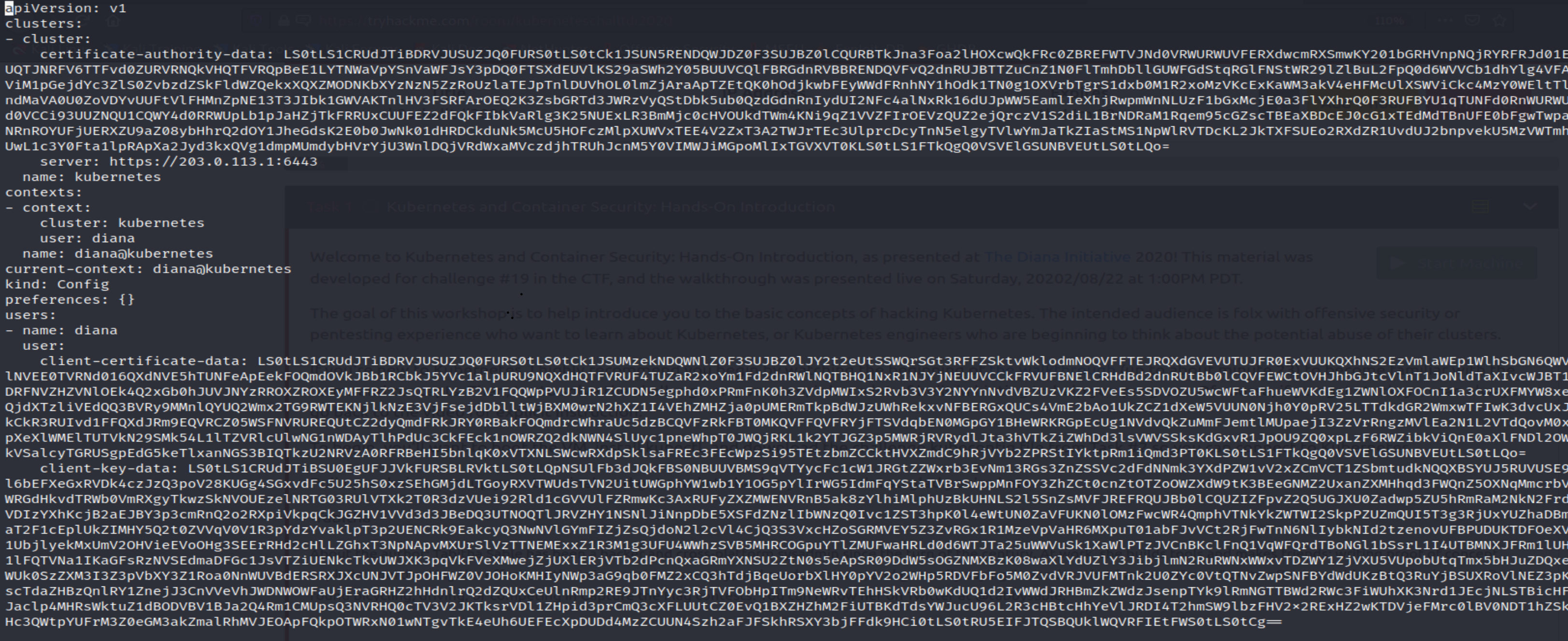
-Tabitha

About the author: Tabitha Sable has been a hacker and cross-platform sysadmin since the turn of the century. At work, she builds tools and makes friends: writing proof of concept exploits, coordinating the efforts of the infrastructure, security, and product teams, and generally saying "I wonder what happens if we..." quite often. Outside of work, she can often be found bicycling, driving, or competing in Capture the Flag contests. You can follow her on Twitter at @tabbysable.

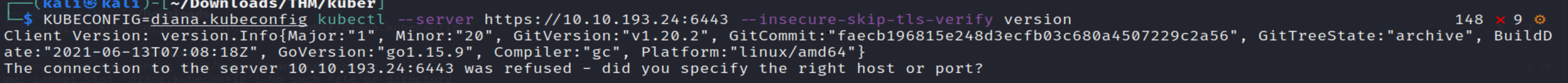
***Answer the questions below***

Use the provided credentials to access the Kubernetes cluster and find the first flag somewhere inside.

Just checking the config file



KUBECONFIG=diana.kubeconfig kubectl --server https://10.10.193.24:6443 --insecure-skip-tls-verify version



https://www.youtube.com/watch?v=n-SJe2PXF\_E

Become cluster admin and find the second flag inside.



 Submit

 Hint

Get the bonus flag from kubernetes.



 Submit

Escape to root on the host and find the third flag.



 Submit

Find the bonus flag on the host.



 Submit

Task 2  Kubeconfig (credential) File Download