Section 1

Cloning the code repository

- git clone https://github.com/devsecops/defcon-workshop.git

Installation / Setting up

A Google Cloud Platform (GCP) account – You can use the GCP Free Tier to get one

- https://cloud.google.com/free/

Linux/Windows software installation instructions

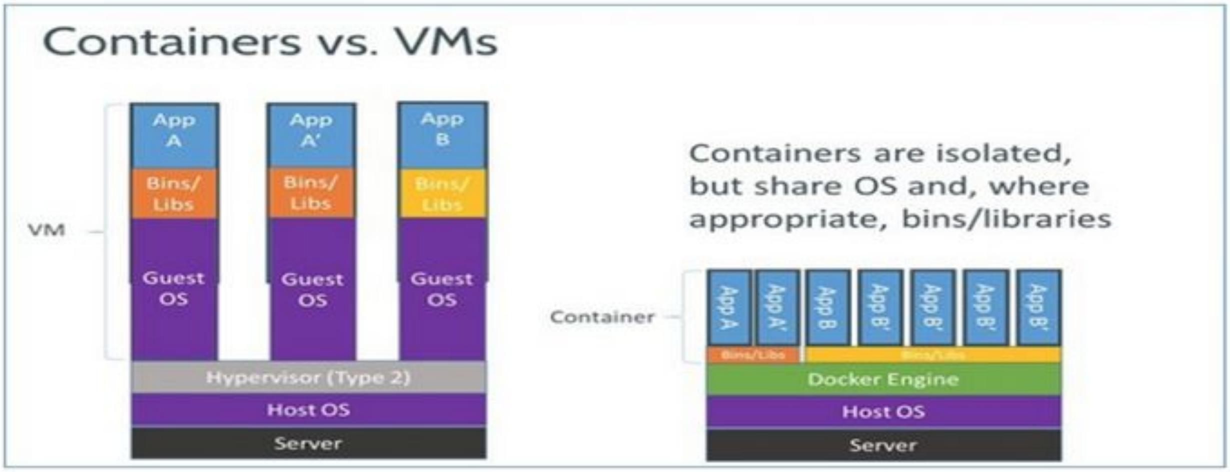
- https://github.com/devsecops/defcon-workshop/tree/master/section-1

Docker

- **Basics**

Think about it like running multiple applications (with varying OS, language) inside a VM but much more lightweight than a VM.

Apps can be run as a Docker containers which are built as Docker images (by writing Dockerfile).



- **Building a Docker image**
  - https://github.com/devsecops/defcon-workshop/tree/master/section-1

- **Pushing the image to GCR**
  - https://github.com/devsecops/defcon-workshop/tree/master/section-1

--
-

Section 2

GCP Web Services

- Google Compute Engine (GCE) - like AWS EC2.
- Google Container Engine (GKE) - Runs containers on a cluster. Entire backend is based on Kubernetes.
- Google BigQuery - Query large amounts of data real quick. Append only.
- Google Cloud Storage (GCS) - like AWS S3.
- Google Container Registry (GCR) - Registry/Repository to store Docker images used in a GCP account
- Google PubSub - Messaging system. Publisher/Subscription model.
    - Publish messages to a topic
    - Create a subscription to that topic
    - Listen for messages on that subscription
    - Acknowledge messages to remove from further consumption

Kubernetes

- **Basics**
    - **http://kubernetes.io/ - Kubernetes is an open-source system for automating deployment, scaling, and management of containerized applications.**
    - **Think about this like an orchestration framework that manages multiple Docker containers and makes sure everything is running smoothly and as per desired configurations communicating with each other**
    - **Takes care of the scaling, service discovery and many other problems that arise in maintaining an infrastructure cluster**
    - **True infrastructure as code**
        - **Can start different moving parts of an infrastructure from YAML files**
        - **YAML files contain the name of the Docker images of the different parts of the infrastructure**

- **Deploying a K8s cluster on minikube**
    - https://github.com/devsecops/defcon-workshop/tree/master/section-2

- **Deploying an alpha K8s cluster on GCP**
    - https://github.com/devsecops/defcon-workshop/tree/master/section-2

--
-

Section 3

Running NMAP on the local K8S cluster

- https://github.com/devsecops/defcon-workshop/tree/master/section-3

Google PubSub in action

- Send a message to a topic
- A topic has one or more subscriptions
- Listen for messages using a subscription
- Acknowledge the message once received

https://github.com/devsecops/defcon-workshop/tree/master/section-3

Convert NMAP data into BigQuery ingest-able format using a Data converter worker

- BigQuery can take only certain data formats. Some common ones include new line delimited JSON and CSV
- NMAP produces output only in certain formats such as xml, normal nmap, greppable and script kiddie
- We need a way to be able to convert nmap's output into BQ ingest-able input
- Converting NMAP's or for that matter any tool's output to CSV seems to be the easiest option as most of the JSON conversion tools don't add new lines, plus nested JSON can get complicated really fast
- So, now, for NMAP's output, we need a way to convert either XML -> CSV or NORMAL NMAP -> CSV. Greppable and script kiddie output are out of the picture
- XML -> CSV = a quick google search yields results about PHP and C#. Nothing solid to do it programatically
- Normal NMAP -> CSV = a quick google search yields a Python script that seems to work fine so we will use this - https://github.com/maaaaz/nmaptocsv

TL;DR - We need a way to be able to generically convert any tool output into CSV or newline delimited JSON to ingest into BigQuery. Until we have a more generic solution that would apply to any tool, we are kind of stuck finding for individual tools for now.

https://github.com/devsecops/defcon-workshop/tree/master/section-3

Querying BigQuery for results data

- https://github.com/devsecops/defcon-workshop/tree/master/section-3

Running Cronjobs

- https://github.com/devsecops/defcon-workshop/tree/master/section-3

Section 4

Standing up vulnerable systems and attack hosts

- https://github.com/devsecops/defcon-workshop/tree/master/section-4

Automation Usecase

- https://github.com/devsecops/defcon-workshop/tree/master/section-4

Automation Usecase with Kubebot

- https://github.com/devsecops/defcon-workshop/tree/master/section-4