Harnessing the Power of Docker and Kubernetes to Supercharge Your Hacking Tactics

Anthony Bislew
Anshuman Bhartiya

Section 1 - Installation / Setting up

- git clone https://github.com/devsecops/defcon-workshop.git
- GCP account - https://cloud.google.com/free/
- Setting up on Windows/MacOS
  - Check Github - https://github.com/devsecops/defcon-workshop/tree/master/section-1

Section 1 - Docker

- Basics
- Building a Docker image
- Pushing the image to Google Container Registry

Section 2 - Google Cloud Platform (GCP) Web Services

- Google Compute Engine (GCE)
- Google Container Engine (GKE)
- Google BigQuery
- Google Cloud Storage (GCS)
- Google Container Registry (GCR)
- Google PubSub

Section 2 - Kubernetes (K8S)

- Basics
- Deploying a K8S cluster locally using Minikube
- Deploying a K8S cluster remote on GCP

Section 3

- Running NMAP on the local K8S cluster
- Google PubSub in action
- Data Converter Worker - convert NMAP output into BigQuery ingest-able format
- Querying BigQuery for results data
- Running Cronjobs

Section 4

- Standing up vulnerable systems and attack hosts
- Automation Usecase
  - Introduction
  - Methodology/Workflow
  - Running locally
  - Running on a cluster
- Automation Usecase with Kubebot - if time permits