Dashboard

Docker Registry

A Docker Registry is used to store and share Docker images among users and systems. Public repositories are mostly protected with authentication. However, in the case of private registries, the users/organizations usually rely on existing security boundaries to protect the registry.
This category deals with insecure Docker registries and attacks that can be done on Docker infrastructure using insecure registries.

What will you learn?

- Interacting with insecure registry with curl
- Fetching images using curl and analyzing image layers
- Attacking protected Docker registry
- Backdooring images and leveraging auto-deployment mechanisms to attack Docker host

References:

1. What is a Docker Registry? (https://docs.docker.com/registry/)
2. Docker registry image (https://hub.docker.com/_/registry)
3. Deploying a Docker registry (https://docs.docker.com/registry/deploying/)

Labs:

- Insecure Docker Registry I
  In this lab, you will learn to interact with an open Docker registry and list images/tags present on it with curl.

- Insecure Docker Registry II
  In this lab, you will learn to fetch a Docker image from an open Docker registry with curl. Then, using tar to extract the different layers and examine the files present on those.

- Protected Docker Registry I
  In this lab, you will learn to launch a dictionary attack on a protected Docker registry. Using the recovered credentials to fetch a Docker image using curl. Extract all layers at once to create the filesystem using tar and examine the extracted files

- Insecure Docker Registry III
  In this lab, you will learn to launch a dictionary attack on a protected Docker registry. Using the recovered credentials to fetch a Docker image using curl. Extract it with tar and examine the files present on different layers.

- Insecure Docker Registry IV
  In this lab, you will learn to fetch a Docker image using curl. Find the order of layers using the manifest file. Extract the layers one by one using tar and examine the files present on different layers. By examining one layer at a time, the overwritten artifacts can be recovered.

- Corrupting Source Image
  In this lab, you will learn to leverage an open Docker registry to steal secret data from a Docker host. A non-exhaustive list of activities to be covered includes:
  - Interact and list images/tags present on the registry using curl
  - Fetch a WordPress image and add a web shell backdoor to it
  - Push the backdoored image to registry
  - Once this infected image is deployed by watchtower, use webshell to steal mounted files from the container

- Corrupting Source Image II

- Interact and list images/tags present on the registry using curl
- Fetch an SSH Docker image and change service port from 22 to 21
- Push SSH image to overwrite the FTP image present in registry
- Once this overwritten image is deployed by watchtower, SSH into it and steal mounted files from the container

- Corrupting Source Image III
  In this lab, you will learn to leverage an open Docker registry to access the files of the Docker host. A non-exhaustive list of activities to be covered includes:
  - Interact and list images/tags present on the registry using curl
  - Fetch an SSH Docker image (with Docker cli in it) and change service port from 22 to 9000
  - Push SSH image to overwrite the Portainer image present in registry
  - Once this overwritten image is deployed by watchtower, SSH into the container
  - Start a new container (with host filesystem mounted on it) on Docker host machine by leveraging the docker socket mounted into the container
  - Use newly created container to access the files of the Docker host

Insecure Docker Registry I

Start

Insecure Docker Registry II

completed all flags verified

Start

Protected Docker Registry I

Start

Insecure Docker Registry III

Start

Insecure Docker Registry IV

Start

Corrupting Source Image

Start

Corrupting Source Image II

Start

Corrupting Source Image III

Start