DOCKER IMAGE ANALYSIS
Docker Image Security

Docker Image Analysis

A Docker image is a file that is used to create a container. It contains applications/binaries and files that define the function and behavior of the corresponding containers. Docker images are built using instructions in a plain-text file known as a Dockerfile.
This category covers the analysis of Docker Image layers and how to recover overwritten artifacts from Docker images.

What will you learn?

- Extracting Docker image layers
- Recovering overwritten artifacts
- Finding secrets from Docker images and using them on live servers

References:

1. Docker Image vulnerability scanning (https://coreos.com/clair/docs/latest/)
2. Docker Image Scanning (https://sysdig.com/blog/docker-image-scanning/)

Labs:

- Hidden Directory
  In this lab, you will learn to leverage the Docker image of a deployed container to steal secrets from the deployed container. A non-exhaustive list of activities to be covered includes:
  - Interact and list images/tags present on the registry using curl
  - Fetch the web server image using curl and extract the images using tar
  - Use the information revealed from previous steps to steal information from running web server container

- Insecure Secret Keys
  In this lab, you will learn to leverage the Docker image of a deployed container to retrieve private keys and then login into the deployed container. A non-exhaustive list of activities to be covered includes:
  - Interact and list images/tags present on the registry using curl
  - Fetch the SSH image using curl and extract the images using tar
  - Look for private key configured for SSH
  - Use this private key to SSH into the running container and steal information from it

- Embedded Credentials
  In this lab, you will learn to leverage the credentials embedded in a Dockerfile that is hosted on an open Git repository to steal secrets from the deployed container. A non-exhaustive list of activities to be covered includes:
  - Interact and check the source files hosted on public Gitlab repository
  - Locate the hardcoded credentials for FTP service
  - Use these credentials to steal information from running FTP container

- Misconfigured Server
  In this lab, you will learn to identify a misconfiguration from the publicly hosted source code of a deployed container and use this misconfiguration to steal secrets from the deployed container. A non-exhaustive list of activities to be covered includes:
  - Interact and check the source files hosted on public Gitlab repository
  - Locate the misconfiguration in web server configuration
  - Use these knowledge to steal information from running web server container