‹ Dashboard

Docker Security Tools

Docker has a rich community of developers, sysadmins and security professionals. This community promotes Docker usage by knowledge sharing, knowledge exchange and creating tools to perform different tasks. There are tools that help in simplifying the management of Docker environments and tools that help in keeping the environment secure.

This category explores the different types of tools that are used for managing and securing Docker ecosystems.

What will you learn?

- Managing Docker with management tools like Portainer
- Performing Docker security audit
- Scanning Docker images for vulnerabilities
- Analyzing Docker images

References:

1. Portainer (https://www.portainer.io/)
2. Scanning Image with Clair (https://coreos.com/clair/docs/latest/)
3. Docker Bench for Security (https://github.com/docker/docker-bench-security)
4. Docker Security (https://github.com/collabnix/dockerlabs/blob/master/advanced/security/ByPassing-Linux-Security-Audit.md)
5. Docker Dive (https://blog.pentesteracademy.com/learn-to-analyze-docker-image-with-dive-tool-4cdee4aeef6b)

Labs:

- Portainer

  In this lab, you will learn to perform various activities using the Portainer tool. A non-exhaustive list of activities to be covered includes:
  - Configuring portainer to use local Docker host
  - List running container
  - View details of the stopped container
  - Check statistics of the running container
  - List the images available on the host
  - Start a container
  - Execute commands on the running container
  - Kill a container
  - Start a stopped a container
  - Start a privileged Container with mounted volume
  - Remove a stopped container
  - Delete unused images
  - List docker networks and docker volumes
  - Viewing event logs of Docker daemon

- Dive

  In this lab, you will learn to analyze a Docker image with the dive tool. A non-exhaustive list of activities to be covered includes:
  - Run dive tool on locally present image
  - Navigate through Dive’s TUI (Terminal based UI)
  - Observe the filesystem at each step of Dockerfile instruction used to create the image
  - Retrieve the artifact

includes:

  - Interacting with Docker Compose UI interface
  - Select and build hello-node project
  - Checking the logs of Docker Compose UI container to understand the working in the backend
  - Interacting with deployed hello-node app

- Seagull
  In this lab, you will learn to perform various activities using the Seagull tool. A non-exhaustive list of activities to be covered includes:
  - List all running and stopped container
  - Start stopped containers
  - List the images available on the host
  - Show information about Docker installation

- Docker Bench Security
  In this lab, you will learn to run Docker Bench Security to locate the misconfigurations/issues with Docker host and running containers. A non-exhaustive list of activities to be covered includes:
  - Run Docker Bench Security script
  - Analyze the output of the script to know about the issues

- Clair
  In this lab, you will learn to scan Docker images with Clair to identify known vulnerabilities present in the image. A non-exhaustive list of activities to be covered includes:
  - Run Clair on a Docker image
  - Analyze the output to know about the vulnerabilities present in the image

- Dockscan
  In this lab, you will learn to run Dockscan to locate the issues with Docker setup. A non-exhaustive list of activities to be covered includes:
  - Run Docscan tool
  - Analyze the output of to know about the issues

- Amicontained
  In this lab, you will learn to run the Amicontained tool visualizing the kind of privileges/capabilities, namespace mappings and runtime a container will get when run with different parameters/arguments. A non-exhaustive list of activities to be covered includes:
  - Run a container without additional parameters and observing results
  - Run a container with pid namespace of host mapped to the container and observing results
  - Run a container with apparmor=unconfined and observing results

- Falco
  In this lab, you will learn to run the Falco tool and observe the malicious actions being detected in its log. A non-exhaustive list of activities to be covered includes:
  - Run Falco and monitor its logs
  - List running containers and cross-reference the list with the Falco logs
  - Exec into one of the running containers and check the corresponding logs
  - Print the contents of /etc/shadow file of the container and check the corresponding logs
  - Create a file in /bin directory of the container and check the corresponding logs

Portainer

⚡ Start

Dive

⚡ Start

Docker Compose UI

⚡ Start