DOCKER FORENSICS
Docker Image Security

Docker Forensics

The Docker ecosystem comprises different components i.e. images, containers, networks, checkpoints, etc. All of these components can be investigated to understand the chain of events in case of an incident. The labs in this section deal with the forensics aspects of Docker components.

What will you learn?

- Extracting artifacts from Docker images
- Locate the backdoors in the running and stopped containers
- Using checkpoints and recover the container state

References:

1. OSQuery and Volatility for Docker Detection and Forensics (http://www.osdfcon.org/presentations/2018/Cem-Gurkok-Docker-Detection-and-Forensics.pdf)
2. Docker Checkpoint (https://docs.docker.com/engine/reference/commandline/checkpoint/)
3. Docker Forensics Toolkit (https://centos.pkgs.org/7/forensics-x86_64/docker-forensics-toolkit-0.2.0-2.el7.x86_64.rpm.html)

Labs:

- Flag File Forensic Recovery I

  In this lab, you will learn to analyze the tar archive of Docker image and retrieve artifacts from it. A non-exhaustive list of activities to be covered includes:
  - Analyze the image history (instruction sequence used in Dockerfile to create it) with container-diff
  - Understand the layer ordering
  - Extract the corresponding layer.tar archive to get the artifact

- Flag File Forensic Recovery II

  In this lab, you will learn to analyze the tar archive of Docker image and retrieve overwritten artifacts from it. A non-exhaustive list of activities to be covered includes:
  - Analyze the image history (instruction sequence used in Dockerfile to create it) with container-diff
  - Understand the layer ordering
  - Extract the corresponding layer.tar archive to get the artifact
  - Understanding that the artifact is overwritten and looking for the original artifact

- System Backdoor

  In this lab, you will learn to identify the changes made to the running container and identify the backdoor added to it. A non-exhaustive list of activities to be covered includes:
  - Identify the changes made to running container using docker diff
  - Locate important files from the modified files
  - Analyze the modified file to identify the backdoor

- Malicious Binary

  In this lab, you will learn to identify the changes made to the running container and identify the backdoor added to it. Then, to analyze the backdoor to understand its working. A non-exhaustive list of activities to be covered includes:
  - Identify the changes made to running container using docker diff
  - Locate important files from the modified files
  - Analyze the modified files to identify the backdoor binary
  - Analyze the backdoor binary using GDB to understand its working

keyboard. A non-exhaustive list of activities to be covered includes:

- Use saved checkpoint to restore the running container to a previous (saved) state
- Dump the process memory of target process
- Analyze the process memory dump to recover the information entered by the user

Flag File Forensic Recovery I

Start

Flag File Forensic Recovery II

Start

System Backdoor

Start

Malicious Binary

Start

Credential Recovery

Start