Docker API Firewall

Docker supports third-party plugins that can be used to enforce custom restrictions on the Docker daemon API. An API firewall can be created by clubbing such plugins together. This is not to be confused with the network firewall that can be created using IPtables.
The labs in this section deal with bypassing or evading the restrictions applied to the Docker daemon REST API using plugins.

What will you learn?

- Bypassing API based restrictions to launch privileged containers
- Learn about JSON structure of Docker API request
- Entering into the running container to perform Docker host compromise

References:

1. Docker REST API (https://docs.docker.com/engine/api/)
2. Docker plugins (https://docs.docker.com/engine/reference/commandline/plugin/)
3. Abusing Docker API leading to RCE (https://www.blackhat.com/docs/us-17/thursday/us-17-Cherny-Well-That-Escalated-Quickly-How-Abusing-The-Docker-API-Led-To-Remote-Code-Execution-Same-Origin-Bypass-And-Persistence_wp.pdf)

Labs:

- Seccomp Unconfined

  In this lab, you will learn to bypass restrictions imposed to disallow privileged containers and get the ability to run commands on the host. A non-exhaustive list of activities to be covered includes:
  - Start a container with seccomp unconfined profile
  - Exec into the container in privileged mode
  - Identify the capabilities available in the container
  - Use SYS_MODULE capability to break out of the container and access host

- Bind Mount I

  In this lab, you will learn to bypass restrictions imposed to disallow mounting host directories (except /tmp) and get the ability to access files of the host filesystem. A non-exhaustive list of activities to be covered includes:
  - Start a container and mount /tmp on it
  - Move bash to it and set setuid on bash binary
  - Run bash binary and get access to host filesystem

- Bind Mount II

  In this lab, you will learn to bypass restrictions imposed to disallow mounting host directories (except /etc) and get the ability to access files of the host filesystem. A non-exhaustive list of activities to be covered includes:
  - Start a container and mount /etc on it
  - Edit shadow file of host (mounted on container) to add root password to it
  - Switch to root user using newly assign password and access host machine

- Unchecked JSON Structure

  In this lab, you will learn to bypass restrictions by sending JSON request to Docker REST API using curl. A non-exhaustive list of activities to be covered includes:
  - Create a container with host filesystem mounted on it by sending curl request
  - Start the already created container
  - Exec into running container then change to mounted directory and access host files

- Leveraging Running Container

- Use curl request to identify Docker TCP socket
- Exec into running container and identify the capabilities
- Use CAP_DAC_READ_SEARCH and CAP_DAC_OVERRIDE to overwrite the shadow file with new root password hash
- SSH into host machine from container to run commands on host machine

- Protected Docker Socket
  In this lab, you will learn to compromise a web application container, steep the bypass token, run a privileged container and break out of the container. A non-exhaustive list of activities to be covered includes:
  - Exploit Wolf CMS and get command execution on the container
  - Steal the bypass token from the container
  - Use this bypass token to start a new container with host filesystem mounted to it (bind mount)
  - Execute reverse shell command in this container and get a reverse connect on attacker machine
  - Use the shell to access files of the host machine

- Unchecked JSON Attribute
  In this lab, you will learn to bypass restrictions to disallow privilege containers and bind mount by sending JSON request to Docker REST API using curl. A non-exhaustive list of activities to be covered includes:
  - Start a container with SYS_MODULE capability using curl request to Docker REST API
  - Use SYS_MODULE capability to insert a reverse shell payload into host machine's kernel
  - Get shell access on host machine

Seccomp Unconfined

Start

Bind Mount I

Start

Bind Mount II

Start

Unchecked JSON Structure

Start

Leveraging Running Container

Start

Protected Docker Socket

Start

Unchecked JSON Attribute

Start