Dashboard

DOCKER MICROSERVICES

Introduction to Containers

Docker Microservices

The ease of deployment of Docker containers has led to increased interest in microservice architecture. This is an approach in which an application is built as a set of loosely coupled, scalable, maintainable, independent services. For example, a WordPress blog on the LAMP stack can be deployed on 2 containers rather than all on one node (machine/container) - the first container will hold the Apache web server and PHP with the WordPress files and the second container will contain the MySQL database.

This section covers attacks on applications that are deployed in the microservice architecture. The attacker will attack the web applications exposed to the internet, get a foothold on the first container, and then use it as a pivot to attack/explore the other containers.

What will you learn?

- Attacking web applications deployed in multiservice architecture
- Pivoting between containers

References:

1. What are microservices? (https://microservices.io/)
2. Guide to deploy containerized microservices (https://docs.microsoft.com/en-us/dotnet/architecture/microservices/)

Labs:

- Attacking Microservice Containers I

  In this lab, you will learn to exploit a web application to get shell access on the container and retrieve the flags. A non-exhaustive list of activities to be covered includes:

  - Scanning the target container with Nmap
  - Exploiting a vulnerable web app with Metasploit to get shell access on the container
  - Discover MySQL credentials and read information kept in tables

- Attacking Microservice Containers II

  In this lab, you will learn to exploit a server misconfiguration to get shell access on the container and retrieve the flags. A non-exhaustive list of activities to be covered includes:

  - Exploiting a web server misconfiguration with Metasploit to get shell access on the container
  - Scan another container connected to web server (but not exposed outside) with Nmap portable
  - Enumerate MongoDB collections to retrieve information

- Attacking Microservice Containers III

  In this lab, you will learn to exploit a server misconfiguration to get shell access on the container and retrieve the flags. A non-exhaustive list of activities to be covered includes:

  - Exploiting a web server misconfiguration with Metasploit to get shell access on the container
  - Scan other containers connected to web server (but not exposed outside) with Nmap portable
  - Launch dictionary attack on protected MongoDB service
  - Enumerate MongoDB collections to retrieve information
  - Interact with Memcached and read the key-value pairs stored in it