Container Security: Beginner Edition Bootcamp

Objective

Though Linux Containers have existed for nearly twenty years, Docker-backed adoption has ensured that containers are now being used in almost all stages of software production i.e. development, testing, and deployment. The flexibility to develop and share applications using Docker and to deploy it at scale using Kubernetes is widely used in the software industry. This makes a sound understanding of container security a vital skill for every security professional.

In this bootcamp, we start with container basics and cover various attack techniques such as container breakouts, privilege escalation, host system compromise, malicious image creation, and cross-container attacks. The learning focus then shifts to securing the different components of this ecosystem and discussing the industry best practices. This bootcamp helps beginners learn essential concepts by encouraging them to try every attack hands-on in our purpose-built labs. As a result, at the end of this bootcamp, you will have the job-ready skills to begin your journey as a Container Security Professional.

Prerequisites

- Basic Knowledge of Computer and Networking
- Familiarity with Linux Operating System

Course Content

Module I: Introduction to Linux Containers

Objective: Learn the basics of Linux containers and how to use Docker to create, manage and run containers. Get an introduction to the Open Container Initiative (OCI) and the various layers of a container system.

1. Container Basics
    a. Basic container principles
    b. How containers differ from virtual machines (VMs)
    c. Namespaces
    d. cgroups
2. Introduction to Docker

   a. Basic commands and concepts
   b. Components i.e. client, daemon, image, container, registry, volume, network
3. Using Docker
   a. Pulling an image
   b. Running a container
   c. Building a container
   d. Pushing a container
   e. Dockerfile
4. Multi-container deployment
   a. Manual setup
   b. docker-compose
5. Introduction to low-level components
   a. containerd
   b. runc

Module II: Attacking Docker Containers

Objective: Understand the threats to a Docker environment with a focus on container privileges, security boundaries and breakouts. Learn about Linux capabilities. Enforce rules and policies with seccomp and AppArmor.

1. Docker security
   a. Threat modeling
   b. Understanding risk vectors
2. Docker container breakouts
   a. Privileged containers
   b. Mounted volumes
   c. Shared namespaces
   d. Additional Linux capabilities
      i. Process injection (SYS_PTRACE)
      ii. Abusing SYS_MODULE capability

Module III: Docker Host Security and Docker Forensics

Objective: Learn how Docker can be exploited to attack the host machine and how to leverage the Docker registry to attack Docker infrastructure. Explore tools and techniques to perform analysis and forensics on different components of Docker such as images and containers.

1. Attacking a Docker host
   a. Mounted Docker socket
   b. World writable socket
   c. Exposed Docker socket

2. Management tools as attack vectors
    a. Portainer
    b. WatchGuard
3. Docker image-based attacks
    a. Insecure Docker Registry
    b. Evil image
    c. Corrupting source image
4. Docker forensics
    a. Analyzing images and exported tar archives
    b. Container forensics
    c. Checkpoints

Module IV: Securing Docker Infrastructure

Objective: Learn about the tools and best practices to secure a Docker environment.

- Securing Docker
    - Auditing socket permissions and Docker group
    - User namespace remapping
    - Auditing runtime
- Monitoring containers
    - Docker events and logs
    - Third-party tools
- Securing Docker images
    - Dockerfile linting and audit
    - Best practices
    - Third-party tools/scanners
- Securing a private registry:
    - Deploying authentication
    - SSL support