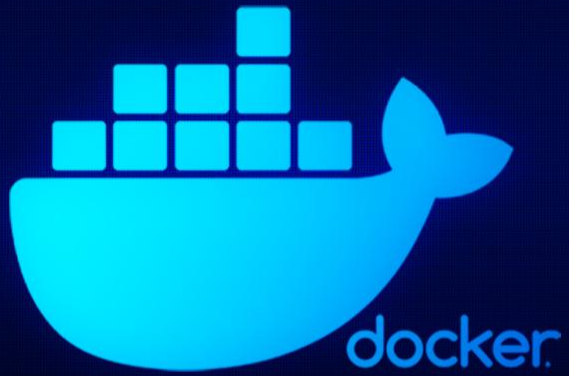
CWL
CyberWarFare Labs

Docker Container Mis-configurations & Escape Webinar



Date : 10th May 2024

CWL Weekly Webinar Series

CyberWarFare Labs

CW Labs is a renowned UK based Ed-tech company specializing in cybersecurity cyber range labs. They provide on-demand educational services and recognize the need for continuous adaptation to evolving threats client requirements.

The company has two primary divisions :

1. **Cyber Range Labs**
2. **Up-Skilling Platform**

About Speaker :

Yash Bharadwaj

Co-Founder & Technical Director at CW Labs UK Pvt. Ltd.

With over **6.5 Years** of Experience as Technologist. Highly attentive towards finding, learning and discovering new TTP's used during offensive engagements.

His area of interest includes **designing, building & teaching** Red / Blue Team Lab Simulation.

Previously he has delivered hands-on red / blue / purple team trainings / talks / workshops at Nullcon, X33fCon, NorthSec, BSIDES Chapters, OWASP, CISO Platform, YASCON etc

You can reach out to him on Twitter **@flopyash**.

Agenda

1.1 Docker 101

1.2 Docker Commands

1.2 Mis-configurations & Exploitation

- Application based
- Configuration based
- Image based

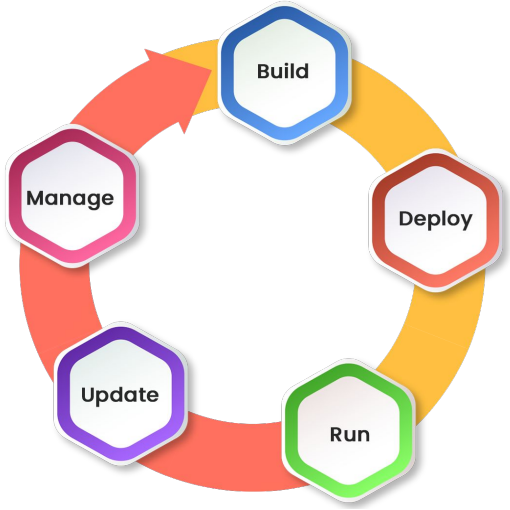
1.3 Case Study

1.4 Defense

1.5 Conclusion

Docker 101

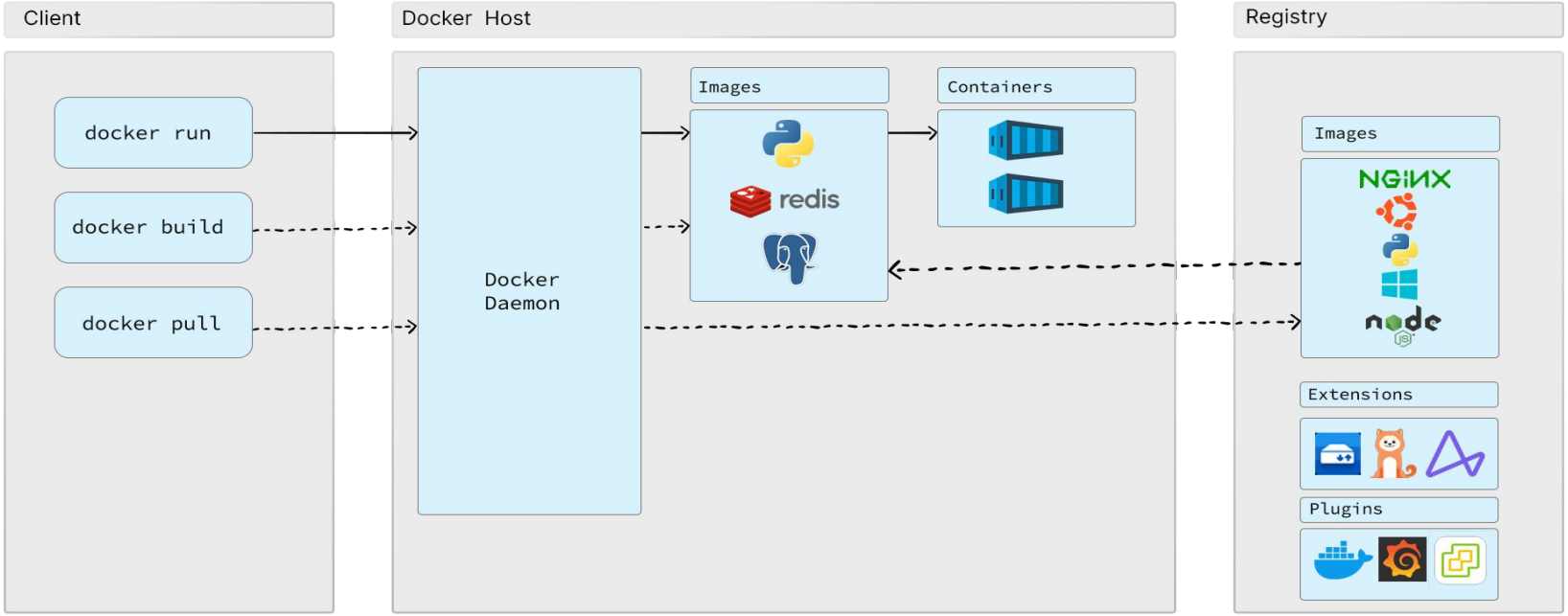
- Released in 2013 as open source project
- Isolated and reusable containers based on customizable images
- Supported Operating Systems include Linux, MacOS, and Windows
- Guided by Open Container Initiative (OCI)
- Available with both CLI and GUI



Docker 101

- Docker objects:
  - **Image**: Image is a basic building block (template) consisting of filesystem and instructions
  - **Container**: Container is a runnable instance of an image
  - **Volume**: Volume is a standalone and persistent storage which can be attached to a container
  - **Network**: Network stack can be configured and attached to a container to enable communication

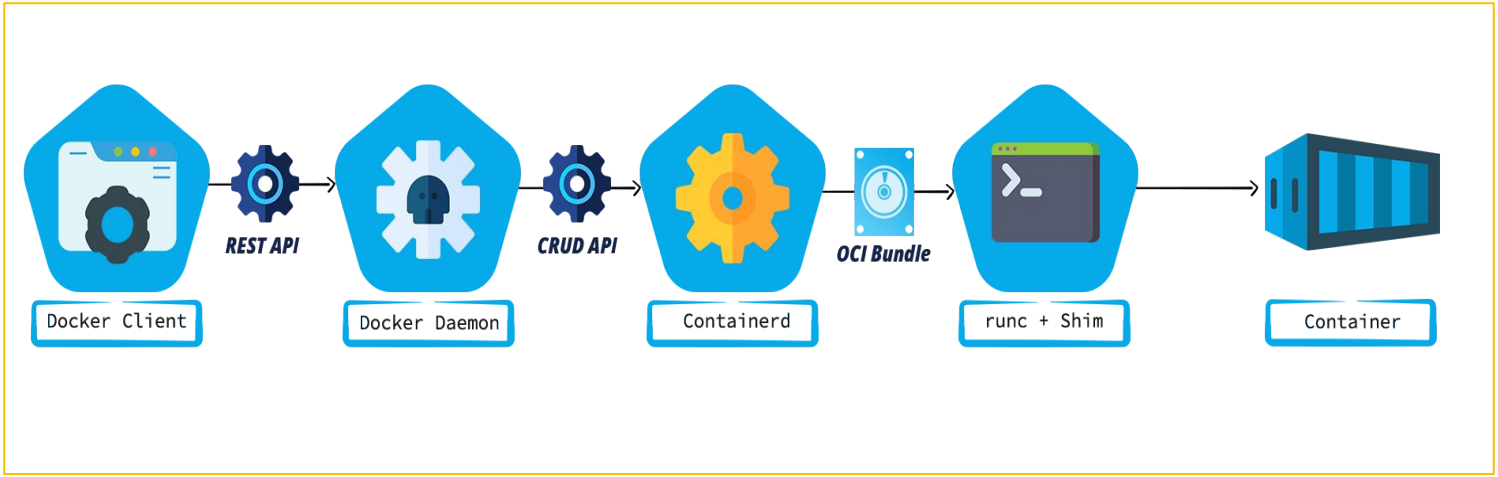
Docker 101



Docker 101

- Docker operates in a Client(**docker**) - Server(**dockerd**) architecture
- Docker Client can be accessed via both the CLI or the GUI (Docker Desktop)
- Client issues commands to the Docker daemon (dockerd) with the help of REST API calls
- Docker daemon executes the requests associated with API calls
- Images are stored in Docker registries

Docker 101



Docker Commands

```
docker pull [OPTIONS] NAME[:tag|@digest]
```

```
docker run [OPTIONS] NAME[:tag|@digest]
```

```
docker ps [OPTIONS]
```

```
docker stop [OPTIONS] CONTAINER [CONTAINER]
```

```
docker start [OPTIONS] CONTAINER [CONTAINER]
```

```
docker build [OPTIONS] PATH | URL | -
```

Docker Mis-configurations

- There are few mis-configurations arises because of :
  - Permissions granted to container
  - Running docker image from untrusted source
  - Host to container configuration
  - Container having access to host network
  - User spawning container added to **Docker** group

DEMO : Initial access to Container

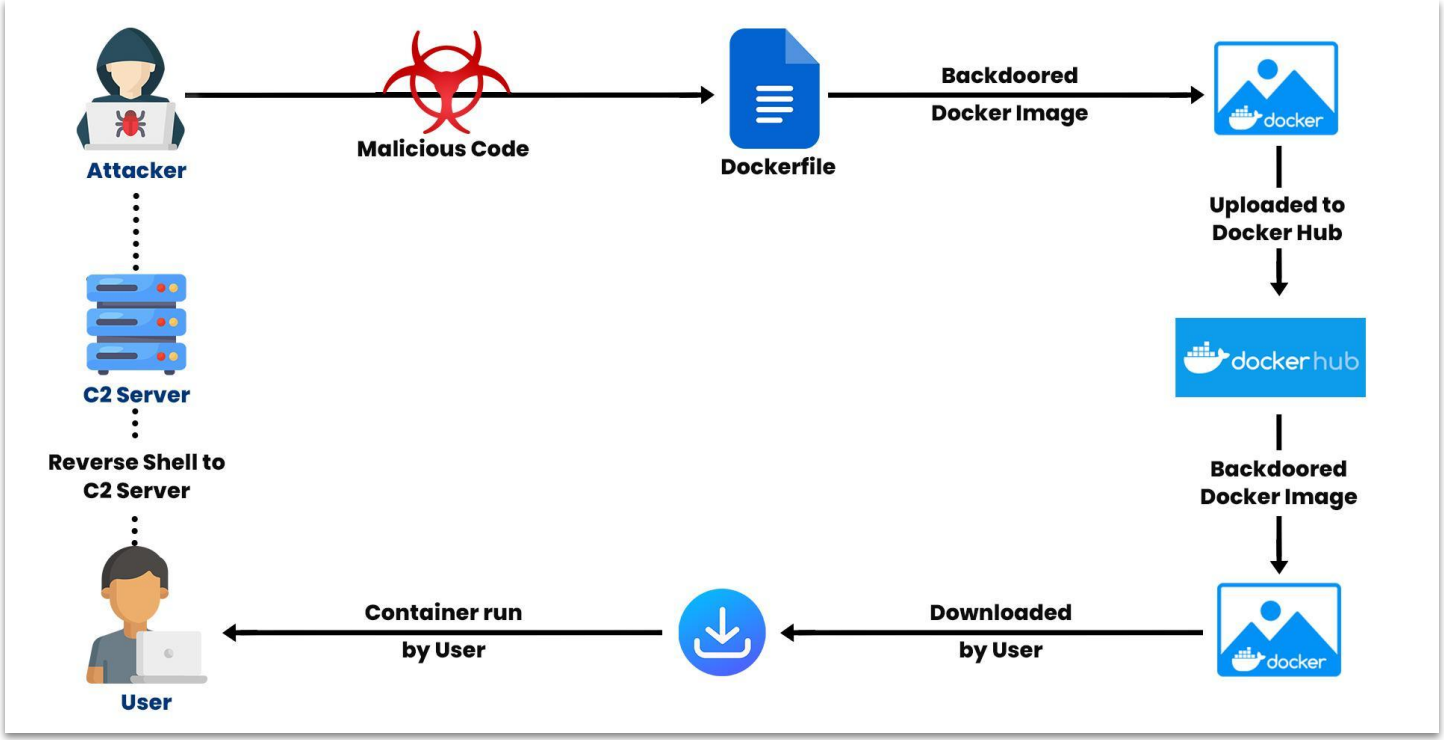
DEMO : Mounted Volume Misconfiguration

Case Study

- Back to basics:
  - Images are the base of any container
  - Images are hosted on publicly/privately available repositories (For e.g, Docker Hub)
  - Anyone can upload their own images
  - Public images can be downloaded (pulled) by anyone

- In past, threat actors have uploaded malicious images of legitimate software on Docker Hub

Case Study



DEMO : Backdoored Docker Image

Docker Defense

- Do NOT allow root user to run container
- Vet Images before pulling from repositories
- Drop all Capabilities and assign only on needed basis
- Include Multi-Stage build via running dockerfile
- Remove unnecessary permissions if not required.

CWL
CyberWarFare Labs

Thank You

For Professional Cyber Penetration Testing / Red Team / Blue Team / Purple Team, Cloud Cyber Range labs / Courses / Trainings, please email

info@cyberwarfare.live

To know more about our offerings, please visit:

https://cyberwarfare.live