WALKOFF SETUP

SECURITY, ORCHESTRATION, AUTOMATION, & RESPONSE (SOAR)

Pre-requisites

Ensure that Docker, Docker Compose 3+, and git are installed!

- Docker CE: https://docs.docker.com/install/#supported-platforms
- Docker Compose: https://docs.docker.com/compose/install/
- Git: https://git-scm.com/book/en/v2/Getting-Started-Installing-Git

If you do not already have a Docker Swarm initialized or joined, run the following command to create one:

```
docker swarm init
```

Note: If you have multiple NICs you will need to use `--advertise-addr` to pick an address from which the swarm will be accessible.

Deploying WALKOFF in a Unix Environment

1. Open a terminal and clone WALKOFF:

```
git clone https://github.com/nsacyber/WALKOFF.git
```

2. Move into the WALKOFF directory:

```
cd WALKOFF
```

3. Build WALKOFF's bootloader container, which handles management of the WALKOFF stack:

- Creating Docker secrets, configs, networks, volumes, etc.
- Building and pushing component images to WALKOFF's internal registry.
- Deploying and removing the Docker Stack.

```
./build_bootloader.sh
```

WALKOFF SETUP

4. Launch WALKOFF with the bootloader, building components as well:

```
./walkoff.sh up --build

# If verbose output is desired:
./walkoff.sh up --build --debug
```

5. Navigate to the default IP and port. The default IP and the port can be changed by altering the port NGINX is exposed on (the right-hand port) in the top-level `docker-compose.yml`. Note that you should use HTTPS and allow the self-signed certificate when prompted.

```
https://127.0.0.1:8080
```

6. The default username is "admin" and password is "admin." These can and should be changed upon initial login.

7. To stop WALKOFF, use the bootloader:

```
./walkoff.sh down

# If removing keys, stored images, and verbose output is desired:
./walkoff.sh down --key --registry --debug
```