Docker Deployment Guide

Installation Guide:

1. **Clone the Caldera Repository:**

   Begin by cloning the Caldera repository recursively (through Git or cmd) to include all submodules:

   ```
   git clone https://github.com/mitre/caldera.git --recursive
   cd caldera
   ```

2. **Convert `download_payloads.sh` to Unix Format:**

   The `download_payloads.sh` script located in the `plugins/emu` directory has Windows-style line endings, which can cause issues in Unix environments. Convert it to Unix format using the `dos2unix` tool:

   ```
   dos2unix plugins/emu/download_payloads.sh
   ```

3. **Modify the Dockerfile:**

   The default Dockerfile uses Python 3.12.x, where the `distutils` module has been removed. To address this, update the Dockerfile to include the `setuptools` package, which replaces `distutils`. Here's how you can modify the Dockerfile:

   - Open the Dockerfile located in the root of the cloned repository.
   - Locate the line that installs Python and related packages:

     ```
     RUN apt-get update && \ apt-get -y install python3 python3-pip
     python3-venv git curl golang-go
     ```

   - Modify it to include `python3-setuptools`:

     ```
     RUN apt-get update && \ apt-get -y install python3 python3-pip
     python3-venv python3-setuptools git curl golang-go
     ```

     This addition ensures that the necessary build and installation tools are available, compensating for the removal of `distutils` in Python 3.12.

   - Updated Dockerfile can be found in the same folder where this deployment guide is.

4. **Create and Configure `local.yml`:**

   Caldera uses configuration files located in the `conf` directory. To customize settings:

- Navigate to the `conf` directory, Copy the default configuration file to create a local version:

-
  ```
  cd conf
  cp default.yml local.yml
  ```

- Open `local.yml` with your preferred text editor and make the following changes:
  - **Update Go and Python Versions:**

    Replace the default Go and Python versions with the desired ones:

    ```
    go: version: 1.22.2 python: version: 3.12.3
    ```

  - **Change User Passwords:**

    Locate the `users` section and update the passwords as needed:

    ```
    users: blue: username: blue password: new_blue_password
    red: username: red password: new_red_password
    ```

    Ensure that the passwords are strong and meet your security requirements.

- local.yml can be found in the same folder where this guide is.

5. **Build the Docker Image:**

   With the modifications in place, build the Docker image:

   ```
   docker build . --build-arg WIN_BUILD=true -t caldera:latest
   ```

   The `WIN_BUILD=true` argument allows Caldera to compile Windows-based agents during the build process.

6. **Run the Docker Container:**

   Start the Caldera server using the newly built Docker image:

   ```
   docker run -p 8888:8888 caldera:latest
   ```

   This command maps port 8888 of the container to port 8888 on your host, allowing access to the Caldera web interface.

7. **Access the Caldera Web Interface:**

   Open your web browser (preferably Chrome or Safari) and navigate to:

   ```
   http://localhost:8888
   ```

Log in using the credentials specified in your `local.yml` file.

Additional Notes:

- **Browser Compatibility:** For the best experience, use Google Chrome or Safari to access the Caldera web interface.
- **Stopping the Docker Container:** To gracefully terminate your Docker container identify the container ID for your running Caldera instance, then stop it:

-
  ```
  docker ps
  docker stop [container ID]
  ```

By following these steps, you will have a customized deployment of MITRE Caldera running in a Docker environment, tailored to your specified configurations.