Docker Compose: Network Security Toolkit

This repository contains a `docker-compose.yaml` file that sets up a Network Security Toolkit with HAProxy, Wireshark, and Security Utilities. The provided `docker-compose.yaml` file creates a custom Docker network and connects all services to it.

Services

1. **proxy** (HAProxy): A high-performance and highly-robust TCP/HTTP load balancer. The configuration file is mapped from the local `haproxy.cfg` file.
2. **wireshark** (ffeldhaus/wireshark): A Docker container running Wireshark with Xpra for remote access. It is connected to the proxy service and uses the same network.
3. **secutils** (michaelborck/secutils): A Docker container containing various security utilities, including Wireshark, nmap, snort, hydra, nikto, wget, curl, ping, netcat, and sqlmap.. It is also connected to the custom network.

Usage

1. Install Docker and Docker Compose.
2. Clone this repository:

```
git clone https://github.com/yourusername/network-security-toolkit.git
```

3. Change to the cloned directory:

```
cd network-security-toolkit
```

4. Create and start the services with Docker Compose:

```
docker-compose up -d
```

Service Configuration

Proxy (HAProxy)

- **IP address**: 192.168.1.2
- **Port**: 14500
- **Configuration file**: `./haproxy.cfg`

Wireshark

- **IP address**: 192.168.1.3

- **Access password**: "wireshark"
- **Captured files**: Stored in the local `./caps` directory

Security Utilities

- **IP address**: 192.168.1.5
- **Port**: 6080
- **Username**: root
- **Password**: rootpassword
- **SSL**: false
- **Data directory**: Mapped to the local `./data` directory

Custom Network Configuration

- **Network name**: custom_network
- **Driver**: bridge
- **Subnet**: 192.168.1.0/24

Stopping and Removing Services

To stop and remove the services, use the following command:

```
docker-compose down
```

Connecting to the Wireshark Container

To access the Wireshark container remotely, follow these steps:

1. Open your web browser and go to `http://localhost:14500`.
2. You will be prompted to enter the Xpra username and password. Use the following credentials:
    - **Username**: wireshark
    - **Password**: wireshark
3. After successful authentication, you will be able to access the Wireshark interface remotely.

Please note that the Wireshark container is connected to the proxy service, which listens on port 14500. Make sure the proxy service is up and running before attempting to connect to the Wireshark container.

Connecting to the Secutils Container

There are two ways to connect to the Secutils container:

Option 1: Command Line Interface

1. Open a PowerShell or terminal window.
2. Run the following command to access the Secutils container's Bash shell:

```
docker exec -it secutils bash
```

3. You can now use the command line tools available within the container, such as Wireshark, nmap, snort, hydra, nikto, wget, curl, ping, netcat, and sqlmap.

Option 2: Graphical User Interface

1. Open your web browser and go to `http://localhost:6080`.
2. Wait a few seconds for the graphical interface to load.
3. you will now have access to the Linux container's graphical interface, where you can use the available security tools.

Remember to ensure that the Secutils container is up and running before attempting to connect using either method.

License