Lab Creation Guide – OWASP Juice Shop with Nginx WAF

1. Installation of Docker

Before starting the lab, Docker must be installed on the host machine.

Prerequisites:

- Windows 10 or Windows 11 system.
- At least 4 GB RAM and 10 GB free disk space.
- Internet connection to download Docker.

Steps to Install Docker Desktop:

- Go to the official Docker website: https://www.docker.com/products/docker-desktop.
- Download Docker Desktop for Windows.
- Run the installer and follow the steps.
- During installation, enable WSL 2 if asked (Windows Subsystem for Linux).
- After installation, restart the computer.
- Open Docker Desktop and check if it is running.

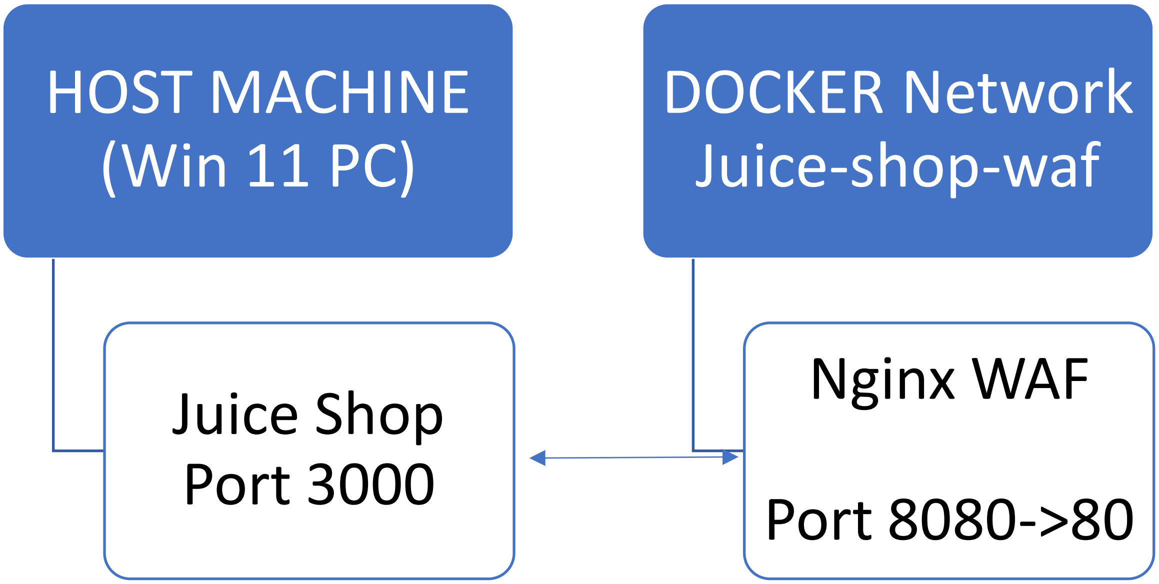
2. Infrastructure Documentation

This lab uses Docker to run two containers:

- Juice Shop: vulnerable web application.
- Nginx WAF: reverse proxy with ModSecurity.

Both containers run on a single host machine (Windows PC with Docker Desktop). They are connected through the default Docker network created by Docker Compose.

3. Network Diagram



Host Machine Ports:

- localhost:3000 → Direct Juice Shop.
- localhost:8080 → Juice Shop through WAF

5. Credentials and Secrets

- Admin account: admin@juice-sh.op with weak password admin123.
- Credentials are stored inside the Juice Shop database. For lab documentation, passwords are shown only for demonstration. In real environments, they should be stored securely and redacted in reports.

6. Setup Steps

- Create a folder C:\Projects\Juice-shop-waf.
- Inside the folder, create files:
- docker-compose.yml
- default.conf
- modsecurity.conf
- crs-setup.conf
- Open PowerShell in the folder and run:
- Verify containers are running using poweahell

Test access:

http://localhost:3000 : Direct Juice Shop.

http://localhost:8080 : Juice Shop through WAF.

7. Versions Used

- Juice Shop Image: bkimminich/juice-shop:latest
- Nginx WAF Image: owasp/modsecurity:nginx
- Docker Desktop: 29.1 or higher
- Docker Compose: v2

Conclusion

This lab guide explains how to set up Juice Shop with Nginx WAF using Docker. It begins with Docker installation, then covers infrastructure documentation, a simple network diagram, configuration files, credential handling, and setup instructions. Following this guide, any student can reproduce the vulnerable environment and perform the attacks described in the attack report.