



Lab Creation Guide

Course: COMP-357: Advanced Pentesting

Instructor: Abe

Student Name: Amirhusen S Shaikh

REDEFINING HACKING

A COMPREHENSIVE GUIDE TO
RED TEAMING AND BUG BOUNTY HUNTING
IN AN AI-DRIVEN WORLD

1. Infrastructure Documentation:

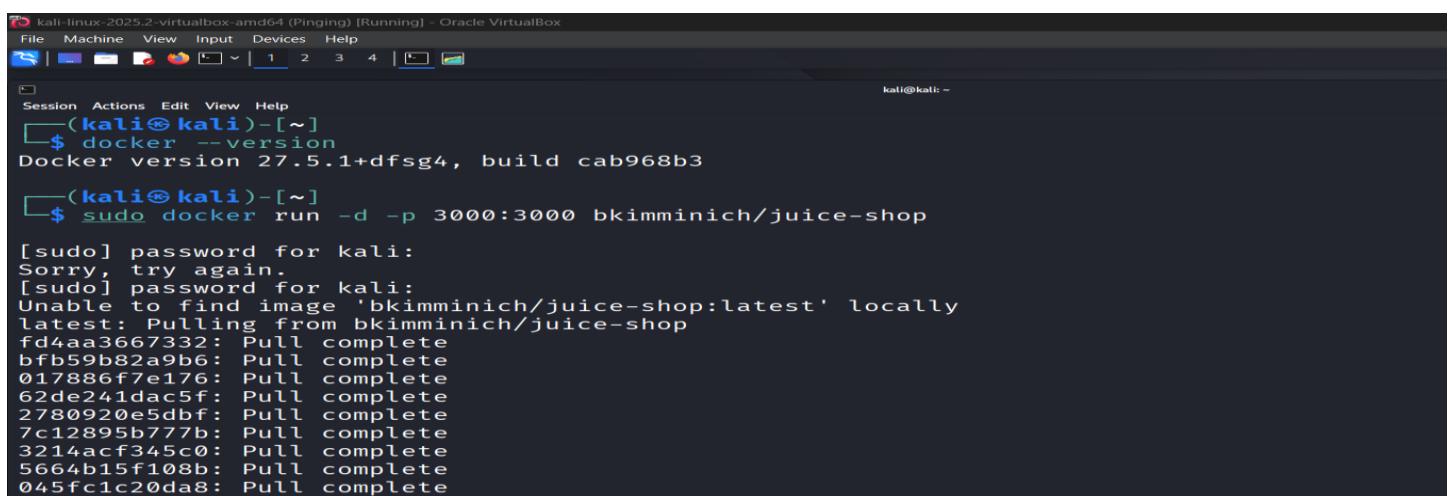
- ✓ **Environment:** Kali Linux 2025.2 VM running in VirtualBox.
 - ✓ **Target Application:** OWASP Juice Shop container.
 - ✓ **Access Method:** Browser on host → <http://localhost:3000>.
 - ✓ **Tools Installed:**
 - **Docker** (For juice shop deployment).
 - **Python3 + venv** (for exploit tool)
 - **Jwt_tool** (For JWT manipulation).
-

2. Network Diagram

- ✓ **Hosts & Segments**
 - Kali VM (Attacker) → Browser + Exploit tools
 - Docker Container (Target) → Juice Shop on port 3000
 - Localhost Nat adapter → forwards traffic from VM to container
 - ✓ **Relevant Ports**
 - **3000/tcp** → Juice Shop web interface
 - **Kali Linux >>> Docker >>> Juice Shop web interface >>> Browser**
-

3. Configuration Files

- ✓ **Docker Run command:**
 - [docker run -p 3000:3000 bkimminich/juice-shop](#)



The screenshot shows a terminal window on a Kali Linux desktop. The terminal output is as follows:

```
kali@kali:~$ docker --version
Docker version 27.5.1+dfsg4, build cab968b3
kali@kali:~$ sudo docker run -d -p 3000:3000 bkimminich/juice-shop
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
Unable to find image 'bkimminich/juice-shop:latest' locally
latest: Pulling from bkimminich/juice-shop
fd4aa3667332: Pull complete
bfb59b82a9b6: Pull complete
017886f7e176: Pull complete
62de241dac5f: Pull complete
2780920e5dbf: Pull complete
7c12895b777b: Pull complete
3214acf345c0: Pull complete
5664b15f108b: Pull complete
045fc1c20da8: Pull complete
```

✓ VM specs:

- OS: Kali Linux (Kali Linux 2025.2) Virtual Box
 - RAM: 4 GB
 - CPU: 2 cores
 - Disk: 20 GB
-

4. Credentials & Secrets

- **User Account:** fixososu@forexzig.com (created in Juice Shop).
 - **JWT Secret:** Weak default (**secret**) discovered during exploit.
 - **Provisioning:**
 - User registered via Juice Shop signup form.
 - JWT was issued automatically on login.
 - **Storage:** JWT stored in browser Local Storage.
 - **Redaction Note:** Password hashes and secrets are documented but redacted in final report.
-

5. Setup Steps

• Prerequisites:

- Kali Linux VM with Docker installed.
- Python3, pip, venv.

• Versions:

- Docker: 27.5.1
- Python: 3.13
- jwt_tool: v2.3.0

- **Steps:**

1. Launch Kali VM.
2. Run Juice Shop container (docker run -p 3000:3000 bkimminich/juice-shop).
3. Access via browser at http://localhost:3000.
4. Register/login with test account. In my case ,I register an account using temp mail. Doesn't have any authentication on mail.
5. Install exploit tooling (git clone https://github.com/ticarpi/jwt_tool.git create venv, install requirements).