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

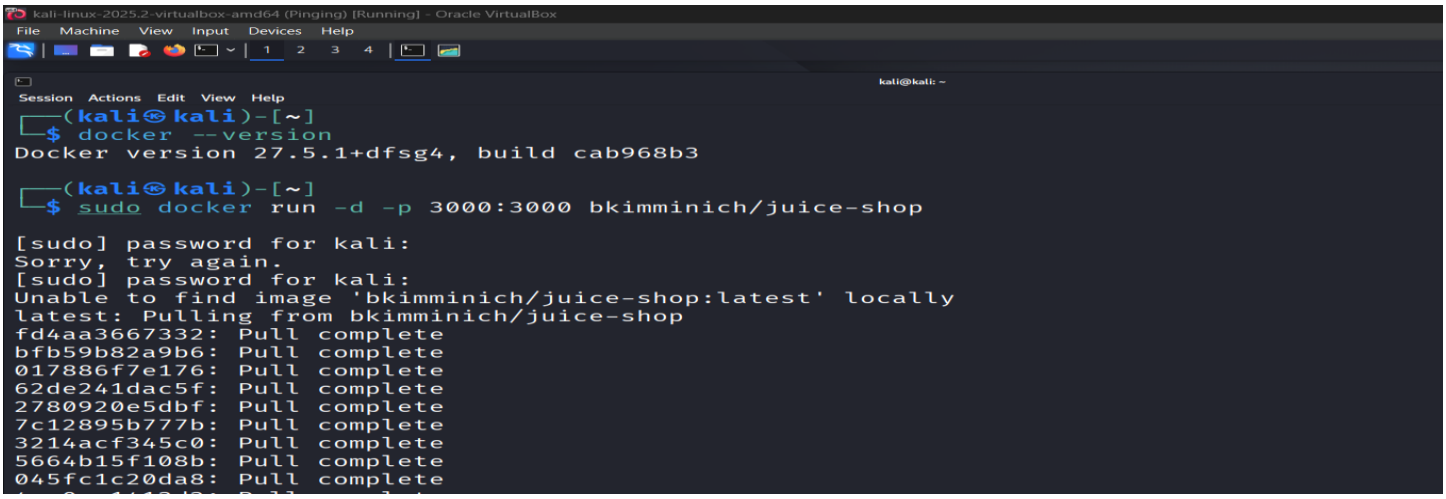
1. **Infrastructure Documentation:**
    - ✓ **Environment**: Kali Linux 2025.2 VM running in VirtualBox.
    - ✓ **Target Application**: OWASP Juice Shop container.
    - ✓ **Access Method**: Browser on host → http://localhost:3000.
    - ✓ **Tools Installed**:
        - **Docker (**For juice shop deployment**).**
        - **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



✓ **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).