COMP – 357

Lab Creation Guide

Submitted by: Sreehari Jiji

Student id: 10316483

Lab Creation Guide

Mega Hacking Project

This guide provides reproducible setup instructions for two independent lab exercises completed in an isolated environment:

- **Exercise 1:** OWASP Juice Shop
- **Exercise 2:** Kerberoasting

All credentials are synthetic and redacted. No external systems or real accounts are used.

Exercise 1 — OWASP Juice Shop Lab Creation Guide

1. Objective

Deploy OWASP Juice Shop in a controlled environment to enable demonstration of common web application vulnerabilities and professional mitigation recommendations.

2. Infrastructure Summary

2.1 Host Platform

- VMware Workstation / Player

2.2 Deployment VM

- Kali Linux

2.3 Container Platform

- Docker Engine

3. Network Design (Exercise 1)

3.1 Host

- Kali Linux VM

3.2 Access

- Juice Shop is accessed locally from the Kali browser.

3.3 Relevant Ports

- HTTP: 3000/TCP

4. Prerequisites

4.1 Kali Requirements

- Kali Linux (recent stable build)
- Internet access for package and image pull during setup

4.2 Install Docker

sudo apt update

sudo apt install -y docker.io

sudo systemctl enable --now docker

5. Configuration Files

5.1 Docker Compose

Stored at: exercise-1-juiceshop/lab-setup/docker-compose.yml

services:

juiceshop:

image: bkimminich/juice-shop:latest

container_name: juiceshop

restart: unless-stopped

ports:

- "3000:3000"

6. Deployment Steps

Location: exercise-1-juiceshop/lab-setup

docker compose pull

docker compose up -d

docker compose ps

7. Validation

Open in Kali browser:

- http://localhost:3000

Setup evidence recommended

- Docker compose file in repository
- Container running output
- Juice Shop homepage with URL visible

8. Credential Handling

- Juice Shop uses its built-in training dataset.
- No real accounts or external authentication are used.

Exercise 2 — Kerberoasting Lab Creation Guide

1. Objective

Build a minimal Active Directory environment to demonstrate Kerberoasting risk against an SPN-linked service account and validate a credential-strength mitigation.

2. Infrastructure Summary

2.1 Host Platform

- VMware Workstation / Player

2.2 Virtual Machines

1. **Domain Controller**
    - Windows Server 2012 R2 Standard Evaluation
2. **Attacker Machine**
    - Kali Linux

3. Network Design

3.1 Segment

- Isolated internal lab subnet: 192.168.45.0/24

3.2 Example IPs used in this lab

- **Domain Controller:** 192.168.45.160
- **Kali:** 192.168.45.133

3.3 Relevant Ports

- **Kerberos:** 88/TCP+UDP
- **LDAP:** 389/TCP+UDP
- **SMB:** 445/TCP
- **DNS:** 53/TCP+UDP

4. VM Specs

4.1 Windows Server 2012 R2

- 2 vCPU
- 2–4 GB RAM
- ~40 GB disk
- 1 NIC on isolated lab network

4.2 Kali Linux

- 2 vCPU
- 2–4 GB RAM
- ~30–40 GB disk
- 1 NIC on the same isolated network

5. Domain Setup Steps (DC)

1. Assign a stable IP on the lab subnet.
2. Install:
    - Active Directory Domain Services
    - DNS Server
3. Promote to a new forest:
    - Domain: lab.local
4. Reboot and verify:
    - AD Users and Computers opens successfully
    - DNS service is running

6. Account & OU Setup

In Active Directory Users and Computers:

1. Create an OU:
    - LAB USERS
2. Create a standard domain user:
    - User1
    - Give a simple password
3. Create a service account:
    - Username: svcweb
    - Display name: Service web
    - Give a simple initial password

7. SPN Configuration

Associate SPN with LAB\svcweb:

- SPN: HTTP/webapp.lab.local

Verify using SPN listing tools on the Domain Controller.

8. Validation Checks

8.1 DC Validation

- Domain lab.local is active
- User1 and svcweb exist under LAB USERS
- SPN verified for svcweb

8.2 Kali Validation

- Can reach the DC on the lab subnet
- Prepared for controlled Kerberos testing

9. Credential Handling

- All credentials are synthetic lab-only identities.

10. Setup Completion Criteria

The Kerberoasting lab is ready when:

- Domain lab.local is operational
- User1 and svcweb are created
- HTTP/webapp.lab.local is confirmed as an SPN for svcweb
- Kali and DC communicate reliably on the isolated network