Comprehensive Penetration Testing Report

Submitted by: Kabsha Farooq

University of Engineering and Technology, Taxila (UET Taxila)

Cybersecurity Internship at Digital Empowerment Network

Date: July 2025

# Task 1: Reconnaissance and Information Gathering

## Objective

To identify publicly available information and enumerate Juice Shop's components using tools like Nmap and browser developer tools.

## Nmap Scan - Host Discovery

I started by checking if the Juice Shop web application is live using a simple host discovery scan.

Command used:

nmap -sn juice-shop.herokuapp.com

Result:

The server is online. IP address received: 54.220.192.176 (with other IPs such as 46.137.15.86 and 54.73.53.134).

## Nmap Scan - Fast Port Scan

I then performed a fast scan to identify the top open ports.

Command used:

nmap -F juice-shop.herokuapp.com

Result:

- Port 80/tcp open (HTTP)  
- Port 443/tcp open (HTTPS)  
- Other 98 ports were filtered (cloud firewall).

This confirms the web application is publicly available on standard web ports and is running behind typical cloud firewall protections.

## Screenshots

The following screenshots are attached:

- Screenshot of Nmap host discovery

- Screenshot of Nmap fast scan with open ports

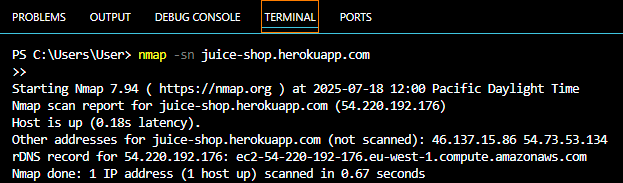


Figure 1: Nmap Host Discovery

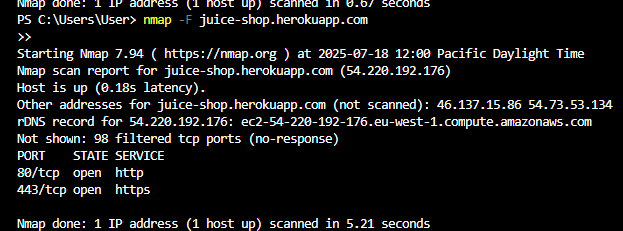
****

Figure 2: Nmap fast scan with open ports