Reconnaissance Report: Juice Shop (https://juice-shop.herokuapp.com)

Executive Summary

This report presents the results of a reconnaissance engagement against the target domain `https://juice-shop.herokuapp.com`. The objectives were to gather publicly available information (passive reconnaissance), enumerate network assets, identify running services, and document potential areas of concern. All tasks were performed ethically, with documentation and screenshots for validation.

Methodology

Tools Used:

- `whois`, `dig` — Domain info and DNS records
- `theHarvester`, `sublist3r` — Email and subdomain collection
- `socialscan` — Username/social profile lookup (install failed)
- `nmap`, `zenmap` — Network enumeration and topology mapping
- Web Browser (Firefox) — Manual review of the target website
- `LibreOffice Writer` — Report compilation

Approach:

1. Conduct passive OSINT against the Juice Shop target domain.
2. Perform internal network scanning and service enumeration.
3. Generate and document a full asset inventory.
4. Report findings with screenshots and observations.

Passive Reconnaissance Findings

WHOIS Lookup:

- No WHOIS server recognized due to Heroku's domain structure.

DNS Records:

- Queried using `dig`. Found NS, CNAME, and RRSIG records for the domain.
- Domain is hosted on Heroku platform and associated with multiple DNSSEC records.

Email & Subdomain Discovery:

- `theHarvester` was run with all sources and limit 300. No email or host data found. API keys for several sources were missing.
- `sublist3r` command failed (`command not found`), indicating tool is not installed.

Social Media Presence:

- Attempted to install and use `socialscan`. Installation failed: "Unable to locate package."

Web Review:

- Attempted to launch Firefox to manually inspect the Juice Shop website. Failed due to root GUI restrictions.

Summary:

- Passive OSINT was limited due to missing tools/API keys.
- No emails or subdomains were found.

Network Enumeration Results

Host Discovery:

- Scanned local network `10.138.16.0/24` using `nmap -sn`
- Identified 2 live hosts:
  - 10.138.16.228 (Apple)
  - 10.138.16.156

Port Scanning:

- Full port scan (`-sS -p-`) against `192.168.1.0/24` revealed no active hosts.

Service Detection:

- Ran `nmap -sV` on `192.168.1.0/24` — no hosts responded

OS Detection:

- Ran `nmap -O` on `192.168.1.0/24` — no hosts responded

Zenmap:

- Installed successfully but screenshots/output not available in this version of the report.

Asset Inventory

IP Address	MAC Address	Hostname	OS	Services Detected
10.138.16.228	C0:95:6D:2E:BC:4C	Unknown	Apple	Unknown
10.138.16.156	Unknown	Unknown	Unknown	Unknown

Potential Vulnerabilities

- Lack of public DNS or email information may indicate hardened OSINT posture.
- Failure to enumerate services or ports could mean hosts are configured with firewalls or scanning is blocked.
- Absence of subdomain and WHOIS information suggests use of dynamic cloud hosting.

Ethical Documentation

All reconnaissance was performed under ethical guidelines and with educational intent.

ACTION	ETHICAL JUSTIFICATION
Passive reconnaissance	Public information only
Port scanning	Authorized network only
Service detection	Non-intrusive scanning

Appendices

- Screenshots of WHOIS, dig, theHarvester, nmap scans, and zenmap installation.
- Raw outputs documented during scan sessions (attached separately or embedded).
