Nmap Exploration & Service Enumeration

2025-10-25

Nmap Exploration & Service Enumeration

Prepared for Applied Information Assurance Projects
Date: October 2025

---

1. Executive Summary

This document summarizes controlled network reconnaissance performed using Nmap in an isolated lab environment. The objective was to identify active hosts, open ports, and service versions; demonstrate safe timing templates and NSE script usage; and produce actionable remediation guidance. All outputs are sanitized for publication.

> **Scope:** Lab subnet `10.200.x.0/24` and Juice Shop test host `10.200.x.42` (sanitized). No external or production systems were scanned.

---

2. Methodology & Scan Profiles

Tools - Nmap 7.x (host discovery, TCP/UDP scans, NSE scripts)
- Optional: `arp-scan`, `ss`, `curl` for verification

Typical commands used (sanitized)

- Host discovery (ping scan):

```
nmap -sn -n 10.200.x.0/24
```

- Quick top-ports + service/version detection:

```
nmap --top-ports 100 -sV -T3 -oA reports/juice-top100 10.200.x.42
```

- Focused web port (Juice Shop default port 3000)

```
nmap -sS -sV -p 3000 -T3 -oA reports/juice-local 127.0.0.1
```

- HTTP enumeration with NSE:

```
nmap -p 3000 --script http-title,http-headers,http-enum -T3 -oN reports/ju
```

- TLS / cipher enumeration:

```
nmap -p 443,3000 --script ssl-enum-ciphers -T3 -oN reports/juice-ssl 127.0
```

Scan timing guidance - Use `-T3` for conservative/safer scans in lab environments. - `-T4` or `-T5` may complete faster but risk service disruption on fragile targets. - Use `--min-rate` carefully; increase only for testbeds designed to handle load.

NSE scripts
- Use targeted NSE scripts (e.g., http-headers, http-title, ssl-enum-ciphers) rather than broad –script vuln unless authorized; the former are largely non-destructive and yield useful metadata.

3. Key Findings (Sanitized)

Severity	Finding	Evidence (sanitized)	Recommendation
Medium	HTTP service running on port 3000 (Juice Shop)	`nmap -sV` shows open port 3000, HTTP response headers present	Use HTTPS for public-facing services; if production, ensure TLS with strong ciphers
Low	Service/version exposure (banners)	`Server: node` / `X-Powered-By` headers present	Remove/obfuscate server banners; minimize information leakage
Low	Missing some security headers	`X-Frame-Options`, `Content-Security-Policy` absent or minimal	Implement HSTS, CSP, X-Frame-Options headers as applicable

> These findings are expected for an intentionally vulnerable test application (OWASP Juice Shop). For production systems, treat medium/above findings as remediation priorities.

4. Sample Sanitized Output

Nmap (sanitized excerpt)

```
# nmap -sV -p3000 127.0.0.1
PORT     STATE SERVICE VERSION
3000/tcp open  http    Node.js (Express)
| http-headers:
|   HTTP/1.1 200 OK
|   Access-Control-Allow-Origin: *
|   X-Content-Type-Options: nosniff
|   X-Frame-Options: SAMEORIGIN
|   Content-Type: text/html; charset=UTF-8
|_  Server: node
```

Interpretation: Service responds with HTTP on port 3000; headers indicate development/test configuration and lack some production-grade security hardening.

5. Risk Interpretation & Prioritization

- **High/Critical:** Only applicable if scanning production systems that show remote code execution or exposed admin interfaces — immediate patching and isolation required.
- **Medium:** Unencrypted services, outdated stacks — schedule patch and TLS rollout.
- **Low:** Banner information and missing headers — remediation during next maintenance window.

Map each finding to NIST CSF: - Identify: Host inventory and service mapping - Protect: Patch management and TLS hardening - Detect: Scheduled scans and SIEM integration - Respond: Remediation tickets and retest cycles

6. Recommendations & Next Steps

1. Run authenticated scans (OpenVAS or credentialed Nmap NSE scripts) only with explicit authorization for deeper checks.
2. Remove or sanitize server banners and X-Powered-By headers where practical.
3. Enforce HTTPS and disable legacy TLS ciphers.
4. Schedule monthly scans and integrate results into a vulnerability tracker.
5. For production, configure alerting in a SIEM and prioritize findings by CVSS.

7. Reproducibility (Commands to re-run in lab)

```
mkdir -p reports
nmap -sn -n 10.200.x.0/24 -oN reports/host-discovery.nmap
nmap --top-ports 100 -sV -T3 10.200.x.42 -oA reports/top100
nmap -sS -sV -p3000 -T3 -oA reports/juice-local 127.0.0.1
nmap -p3000 --script http-title,http-headers -T3 -oN reports/juice-http-in
```

8. References & Tools

- Nmap documentation: https://nmap.org
- OWASP Juice Shop: https://owasp.org/www-project-juice-shop/
- NIST SP 800-115: Technical Guide to Information Security Testing and Assessment

Download Report (PDF)

```
```