# Task 3 — Expanded Vulnerability Scan Documentation (Simulated)

## README

```
# Task 3 — Basic Vulnerability Scan (Simulated)
This repository contains a simulated vulnerability scan using Nessus/OpenVAS.
```

# Simulated Vulnerability Scan Report

```
# Vulnerability Scan Report (Simulated)
## Executive Summary
A simulated full vulnerability scan was performed on a local machine. This report summarizes identified issues.
```

# Simulated Raw Scan Output

```
Simulated Scan Results:
- Open Ports: 22, 80, 139, 445
- Vulnerabilities:
  - SSH Weak Algorithms (Medium)
  - SMB Signing Not Required (Medium)
  - Outdated Apache Server (Low)
```

# Methodology

```
# Methodology
This simulated vulnerability assessment follows a standard structure:
1. **Reconnaissance** – Identifying open ports and exposed services.
2. **Scanning** – Running a full vulnerability scan using a security scanner.
3. **Analysis** – Reviewing vulnerability classifications and CVSS scores.
4. **Reporting** – Documenting findings with recommendations.
```

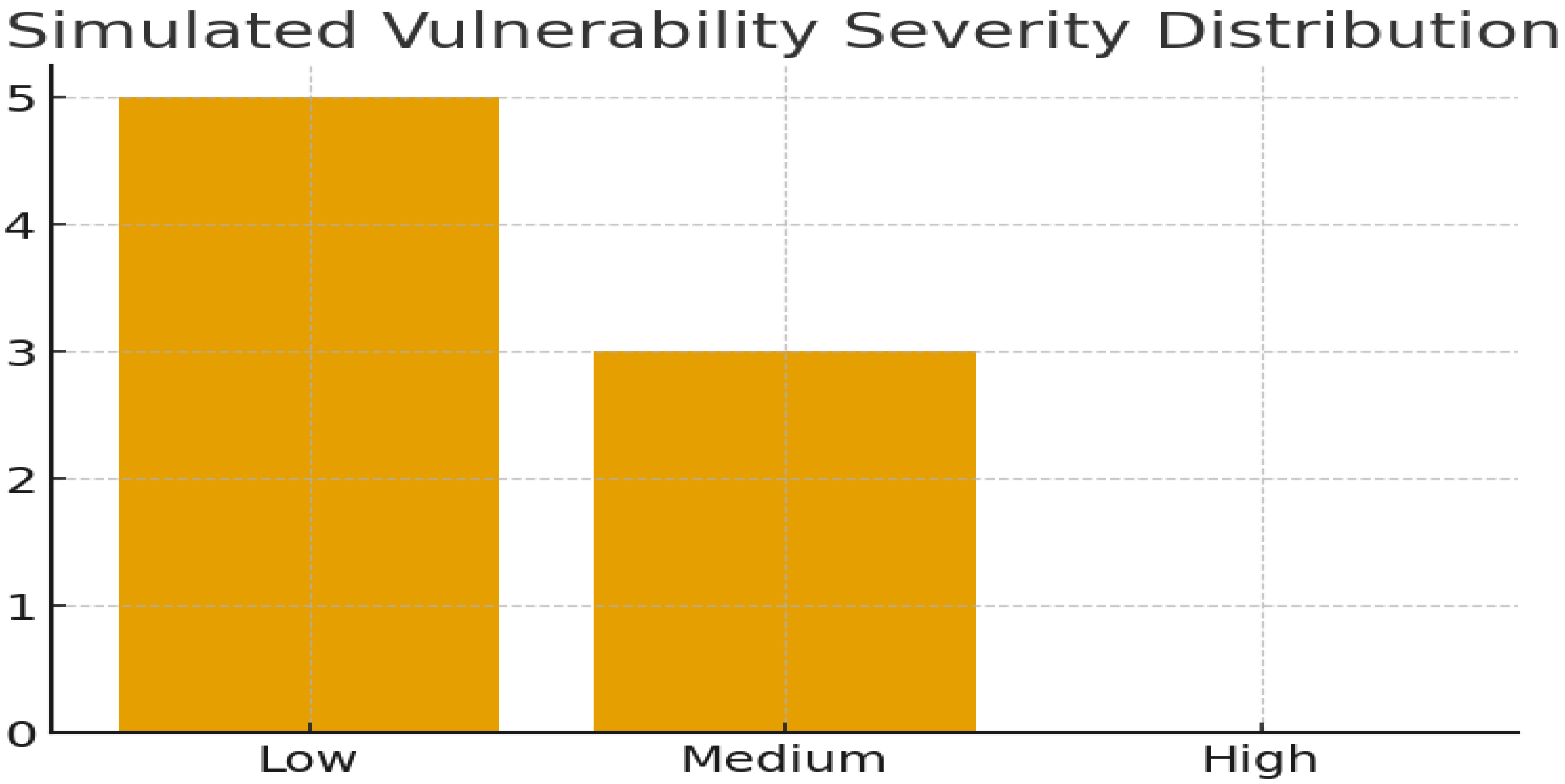
# CVSS Overview

```
# Understanding CVSS
CVSS (Common Vulnerability Scoring System) categorizes vulnerabilities based on severity:
- **Low (0.1 – 3.9)** — Minor risks with limited impact.
- **Medium (4.0 – 6.9)** — Moderate risk; attackers may exploit weak configurations.
- **High (7.0 – 8.9)** — Serious exposure requiring urgent remediation.
- **Critical (9.0 – 10)** — Severe issues actively exploitable by attackers.
```

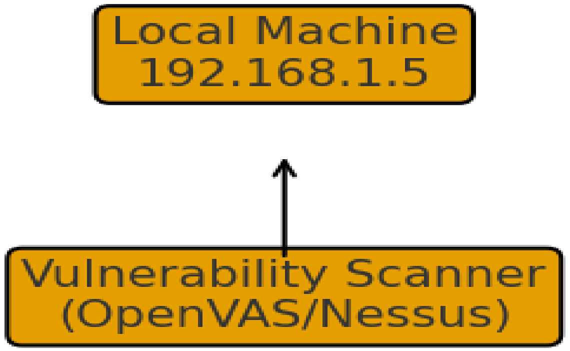
# Recommendations

```
# Recommendations
Based on simulated findings:
- Update outdated services like Apache HTTPD.
- Enforce SMB Signing.
- Disable weak SSH algorithms.
- Apply OS and security patch updates regularly.
- Use a firewall to restrict unnecessary services.
```

## Severity Overview Chart



## Scan Architecture Diagram


Local Machine
192.168.1.5
Vulnerability Scanner
(OpenVAS/Nessus)