1. Introduction

This report documents the results of network scanning and enumeration performed using Nmap and Nessus Essentials. The objective was to identify open ports, running services, and potential vulnerabilities on the target system (localhost). The findings include raw scan results, service enumeration, vulnerability assessment, and recommendations for mitigation.

---

2. Port Scanning Analysis

2.1 TCP SYN Scan (`nmap -sS -p- -v localhost`)

- **Scan Type:** SYN Stealth Scan (TCP)
- **Results:**
  - All 65,535 ports were scanned.
  - No open TCP ports detected (all in a closed/reset state).
  - **Implication:** No services were actively listening on TCP ports, or a firewall blocked the connections.

2.2 UDP Scan (`nmap -sU -p- -v localhost`)

- **Scan Type:** UDP Scan
- **Results:**
  - Port **123/UDP (NTP)** was found open.
  - All other 65,534 ports were closed or unreachable.
  - **Implication:** The system is running an NTP service, which may be vulnerable to attacks like NTP amplification.

2.3 Service Version Scan (`nmap -sV -p- -v localhost`)

- **Scan Type:** Service Version Detection
- **Results:**
  - No open TCP services detected.
  - Nmap attempted service detection but did not identify any running services.
  - **Implication:** Either no services were running on common TCP ports, or security controls prevented service detection.

---

3. Vulnerability Scanning (Nessus Essentials)

3.1 Key Findings from Nessus Scan

- **Open Ports Identified:**
  - **Port 67/UDP** (DHCP Server Detection) - Low Risk
  - **Port 80/TCP** (HTTP Service) - No risk reported
  - **Port 123/UDP** (NTP Server Detection) - No risk reported
  - **Port 5400/TCP** (Unspecified Service) - No risk reported
- **Potential Security Risks:**
  - **NTP Server (Port 123/UDP):** May be vulnerable to NTP reflection or amplification attacks.
  - **DHCP Server (Port 67/UDP):** Exposure may allow attackers to gather network configuration details.
  - **Traceroute Information Leak:** Could be used for network reconnaissance.
  - **Open HTTP Port (80/TCP):** If improperly configured, may expose sensitive information.

---

4. Correlation of Nessus and Nmap Findings

Port	Protocol	Service Detected by Nmap	Service Identified by Nessus	Risk Level
67	UDP	Not detected	DHCP Server Detected	Low
80	TCP	Not detected	HTTP Service Detected	None
123	UDP	Open (NTP)	NTP Service Detected	None
5400	TCP	Not detected	Open Port Found by Nessus	None

Discrepancies and Possible Explanations

- Nmap and Nessus both confirm an **NTP service running on UDP port 123**.
- Nessus identified **ports 67 (DHCP), 80 (HTTP), and 5400 (TCP) as open**, but they were not detected as open by Nmap.
- **Possible reasons for discrepancies:**
  - Nmap may not have had privileges to scan certain ports.
  - Nessus performs deeper protocol-based service detection.
  - A firewall may have blocked Nmap's scanning attempts.

---

5. Verification and False Positive Analysis

- **Validate Nessus findings** using manual testing (`netstat` or `ss` commands).
- **Check firewall rules** to confirm whether certain ports are being blocked.
- **Re-run scans with different configurations** to verify discrepancies.

---

6. Recommendations and Mitigation Strategies

1. **Restrict Unnecessary UDP Services**:
    - Disable or secure the NTP service if not needed.
    - Block public access to the DHCP server unless required.
2. **Close Unused Ports**:
    - Implement firewall rules to allow only necessary services.
3. **Secure HTTP Service (Port 80)**:
    - If a web service is running, ensure HTTPS is enforced.
    - Remove unnecessary or test pages that may leak information.
4. **Limit Traceroute Exposure**:
    - Apply firewall rules to prevent unauthorized ICMP or UDP traceroutes