Vulnerability Assessment Report – My Basic Network Scan

## 1. Objective

To perform a basic vulnerability assessment of a local machine using Nessus Essentials. Aimed at introducing to real-world vulnerability scanning and risk assessment using industry-standard tools.

## 2. System & Scan Details

* Tool Used: Nessus Essentials
* Scan Policy: Basic Network Scan
* Scan Status: Running (99% complete)
* Scan Target: Local IP - 192.168.248.12
* Scanner Type: Local Scanner
* Scan Start Time: 10:17 AM
* Reported At: 10:25 AM, June 1, 2025
* CVSS Version: 3.0

# 3. Summary of Results

Total Hosts Scanned: 1  
IP Address: 192.168.248.12  
Total Vulnerabilities Detected: 60

* Medium Severity: 2
* Low Severity: 58
* High/Critical: 0 (at this stage of the scan)

Visualization (based on screenshot):  
- The vulnerability pie chart indicates the vast majority (approx. 97%) are of low severity.  
- Medium severity issues are minimal (approx. 3%).

# 4. Initial Observations

The system appears free from high or critical vulnerabilities, which is a positive indicator.  
However, 58 low severity issues suggest several configurations or software packages may require optimization or patching.  
The presence of 2 medium severity vulnerabilities means there are still moderate risks that need attention.

# 5. Reflections

This exercise provided hands-on experience in:

* Using Nessus Essentials for vulnerability scanning.
* Interpreting scan outputs and CVSS-based severity ratings.
* Beginning the remediation cycle for system hardening.

It emphasized the importance of continuous monitoring and secure system configurations in cybersecurity practices.