Vulnerability Assessment Report

1. Introduction

This vulnerability assessment was conducted to identify open services and potential security risks on a target host within a local network. The assessment was performed using Nmap, a widely used network scanning tool, to enumerate open ports and running services.

2. Scope of Assessment

Target IP: 192.168.88.23
Network Type: Local Area Network (LAN)
Tool Used: Nmap 7.95
Date: 20 December 2025

3. Scan Summary

The scan identified four open TCP ports while most other ports were filtered, indicating firewall activity.

4. Identified Open Ports

135/tcp (MSRPC) – Medium Risk
Used by Windows services and can be abused for system enumeration.

139/tcp (NetBIOS) – Medium Risk
Legacy Windows file-sharing service vulnerable to enumeration.

445/tcp (SMB) – High Risk
Common attack vector used in ransomware and lateral movement.

5357/tcp (WSDAPI) – Low to Medium Risk
Used for device discovery, increases attack surface.

5. Risk Assessment

Overall system risk is assessed as Medium to High due to exposed SMB and NetBIOS services.

6. Recommendations

- Restrict ports 135, 139, and 445 using firewall rules.
- Disable NetBIOS if not required.
- Keep the system fully patched.
- Monitor logs for suspicious activity.

7. Conclusion

The assessment identified multiple exposed services that increase attack surface. Applying recommended security controls will significantly improve system security.