Network Vulnerability Scan Report

Conducted by: Daniyal

SAP ID: 27670

Tool Used: Nessus

Scan Title: My Basic Network Scan

Scan Date: 5/May/2025

Executive Summary

This report provides a comprehensive overview of the results from a network vulnerability scan performed using Nessus...Recommendations are provided for mitigating the identified vulnerabilities.

Scan Overview

Scan Type: Basic Network Scan

Plugin Set: Nessus Default

Total Hosts Scanned: 1

Total Vulnerabilities Found: 28

Scan Duration: 2 minutes

Target Information

IP Address / Host: 192.168.1.10

Operating System: Windows 10 Professional

Open Ports: TCP 80, 135, 139, 445, 3389

Detected Services: Microsoft SMB, Remote Desktop, HTTP Server, RPC

Vulnerability Summary

Critical: 2

High: 6

Medium: 10

Low: 5

Informational: 5

Detailed Findings

1. Microsoft Windows SMBv1 Vulnerability (Critical)

Description: The target is running SMBv1, which is deprecated...

Solution: Disable SMBv1 and apply patches.

2. Remote Desktop Protocol Server Man-in-the-Middle Weakness (High)

Description: RDP allows unencrypted connections...

Solution: Enable NLA and restrict RDP access.

3. Microsoft Windows OS Outdated Patch Level (Medium)

Description: Host is missing patches.

Solution: Regularly update OS.

4. SSL Certificate Expiry (Informational)

Description: SSL cert is near expiry.

Solution: Renew SSL cert.

Recommendations

- Disable SMBv1

- Regularly patch systems

- Harden services

- Implement monitoring

- Enforce strong policies

Conclusion

The scan identified several vulnerabilities. Immediate remediation is required for critical issues. Following the recommended actions will improve the network's security.