# Executive Summary – Vulnerability Assessment & Penetration Testing

Objective:  
To assess the security posture of the Windows 10 and Debian Linux systems and identify potential vulnerabilities that could lead to compromise.

## Key Findings Summary

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| System | Critical Issues | High | Medium | Low |
| Windows 10 | 1 | 2 | 3 | 1 |
| Debian Linux | 0 | 3 | 2 | 2 |

## Top Risks Identified

- Windows 10: SMBv1 protocol enabled – exposes system to WannaCry-style attacks.

- Debian Linux: Unpatched Apache HTTP Server vulnerability (CVE-2021-41773).

- Both systems: Weak or default passwords detected.

## Areas of Improvement

- Disable legacy services like SMBv1.

- Enforce patch management policies.

- Implement strong password policies and enforce MFA.

- Monitor logs and set up alerts for suspicious activities.

## Business Risk If Exploited

If left unresolved, these vulnerabilities could lead to unauthorized access, data breaches, service disruptions, or complete system compromise, leading to financial and reputational damage.