Vulnerability Assessment Report

Prepared by: Rizwan Khurram

Date: July 22, 2025

Vulnerability: Outdated OpenSSH Detected

Risk Level: High

Details: The target is running OpenSSH 7.2, which contains multiple known vulnerabilities.

Recommendation: Upgrade to OpenSSH version 9.0 or later.

Vulnerability: SSL Certificate Expired

Risk Level: Medium

Details: The SSL certificate expired on Jan 15, 2024. This could impact trust and encryption.

Recommendation: Renew the SSL certificate with a valid CA.

Vulnerability: Anonymous FTP Access Enabled

Risk Level: Low

Details: FTP server allows anonymous login. This could expose files unintentionally.

Recommendation: Disable anonymous access or secure the FTP configuration.