🔐 Vulnerability Assessment Report – OpenVAS (Greenbone Security Assistant)

# 🧰 Tool Used:

- Tool: Greenbone Security Assistant (OpenVAS)

- Platform: Kali Linux

- Scan Type: Full and Fast

# 🎯 Target:

- IP Address: 127.0.0.1 (Localhost)

- Scanned Port: 5432/tcp

# 🧪 Scan Summary:

- Total Vulnerabilities Found: 1

- Critical: 0

- High: 0

- Medium: 1

- Low: 0

# 🚨 Most Crucial Vulnerability

## Vulnerability Name:

SSL/TLS: Report Weak Cipher Suites

## CVSS Score:

5.9 (Medium)

## Affected Host:

- IP Address: 127.0.0.1

- Port: 5432/tcp

## Description:

The SSL/TLS service on the target system is configured to support cipher suites that are considered weak. These weak cipher suites can allow attackers to potentially decrypt or manipulate encrypted communication, leading to security breaches.

# 🛠️ Solution / Mitigation:

To mitigate this vulnerability:

- Disable weak SSL/TLS cipher suites on the server.

- Enforce modern encryption standards such as TLS 1.2 or TLS 1.3.

- Avoid deprecated algorithms including: RC4, 3DES, Export-grade ciphers.

- Update or reconfigure the SSL/TLS settings in your server software (e.g., PostgreSQL, Apache, Nginx, etc.).

- Restart the affected service after applying changes.

# 🔍 References:

- OWASP Transport Layer Protection Cheat Sheet: https://cheatsheetseries.owasp.org/cheatsheets/Transport\_Layer\_Protection\_Cheat\_Sheet.html

- Mozilla SSL Configuration Generator: https://ssl-config.mozilla.org/

# 📸 Screenshot of Vulnerability:

\*(Insert the screenshot below this text – you can paste the image directly into the Word document or insert it via “Insert > Picture”)\*

# 📁 Included Attachments:

- This Word report (.docx)

- Screenshot of the vulnerability

- (Optional) Exported report in .pdf from Greenbone

# ✅ Submission Note:

This documentation was prepared as part of the Cyber Security Internship – Task 3: "Basic Vulnerability Scan using OpenVAS."