Vulnerability Scan Report

Name: Rudraksh Kaushik Task: Basic Vulnerability Scan on local PC Tool used: Nessus Essentials (or OpenVAS/GVM) Scan date: 2025-11-17

1. Scan summary

- Target: localhost (127.0.0.1) or IP: 192.168.x.x
- Scan type: Full network/basic network scan
- Total vulnerabilities found: X
  - Critical: A
  - High: B
  - Medium: C
  - Low: D

2. Most critical findings (top 5)

1. CVE-XXXX-XXXX — [Vuln name]
   - Severity: Critical
   - Description: short line
   - CVSS: 9.8
   - Recommendation: apply patch / disable service / update software
2. CVE-YYYY-YYYY — [Vuln name]
   - Severity: High
   - Recommendation: update package / change config

(Repeat for top 3–5)

3. Remediation steps (simple)

- Keep OS updated (Windows Update / apt update & upgrade)
- Remove or update vulnerable software
- Close unnecessary open ports
- Use strong passwords and services with latest patches

4. Tools & commands used

- Nessus Essentials (UI)
- or OpenVAS/GVM (`sudo gvm-setup`, web UI at https://localhost:9392`)

5. Files included

- nessus_report.pdf
- screenshots/email/scan-config.png
- report.pdf

6. Conclusion

This scan shows common issues and basic fixes. For production, do repeated scans and patch management.