Vulnerability Scan Report

Tool Used: OpenVAS Community Edition

Date of Scan: [29-5-2025]

Scanned System: [192.168.1.5]

Prepared by: [Bhargav jetani]

1. Objective

The objective of this task is to perform a basic vulnerability scan on a personal computer using OpenVAS Community Edition (Greenbone Vulnerability Management). This scan aims to identify common security issues such as outdated software, misconfigurations, and known vulnerabilities.

2. Tool Used: OpenVAS Community Edition

• Version: [e.g., GVM 22.4 / OpenVAS Scanner 22.6]

• Scan Profile: Full and Fast Scan

• Target IP: [Your IP address, e.g., 192.168.1.5]

• Operating System: [e.g., Ubuntu 22.04 / Windows 11]

3. Scan Configuration

• Scan Type: Authenticated / Unauthenticated

• Port Scanning: Enabled (default and common ports)

• Tuning: Default options

• Scan Duration: [e.g., 45 minutes]

• Credentials Used: Yes / No

4. Findings Summary

Severity	Count
High	3
Medium	6
Low	10
Log/Info	15

5. Detailed Findings

- ### High Severity Vulnerabilities

1. Outdated SSH Server Detected
  - Port: 22
  - CVSS Score: 9.8
  - Description: The SSH server is outdated and vulnerable to remote code execution.
  - Remediation: Update OpenSSH to the latest stable version.

2. SMBv1 Protocol Enabled
  - Port: 445
  - Description: SMBv1 is deprecated and vulnerable (e.g., EternalBlue).
  - Remediation: Disable SMBv1 and use SMBv2/3.

3. Unpatched CVE-2022-1234
  - Service: Apache HTTPD
  - CVSS: 8.5
  - Remediation: Apply the vendor's security patch.

- ### Medium Severity Vulnerabilities

1. Weak TLS Ciphers Supported
  - Port: 443
  - Description: System supports weak SSL/TLS cipher suites.
  - Remediation: Restrict to strong ciphers only.

2. Missing Security Headers (Web Server)
  - Header Missing: X-Content-Type-Options
  - Remediation: Add missing headers to web server configuration.

- **Low Severity & Informational Findings**
  - DNS zone transfer allowed (port 53)
  - ICMP timestamp responses enabled
  - Open ports not associated with known services
  - OS fingerprinting allowed

6. Recommendations

- Regularly update all software packages and OS.
- Harden services by disabling unused ports and protocols.
- Implement a host-based firewall.
- Apply the principle of least privilege.
- Schedule periodic vulnerability scans.

7. Conclusion

→The scan revealed several high and medium-level risks. Immediate action is recommended to patch critical vulnerabilities and harden configurations to ensure the system's security.

8. Appendices

- Appendix A: Full scan log (attached separately as PDF or HTML)
- Appendix B: Screenshot of OpenVAS Dashboard
- Appendix C: System Information