Vulnerability Scan Report - OpenVAS

1. Target Details:

Attacker Machine: Kali Linux

Victim Machine: Windows 10 Virtual Machine

Target IP: 192.168.163.129

Scanner Used: OpenVAS (Greenbone Community Edition)

Scan Type: Full and Fast

Scan Duration: ~45 minutes

2. Scan Summary:

- SMBv1 Enabled (CVE-2017-0144) - High Severity - CVSS: 9.8
  Description: Legacy protocol still active. Vulnerable to WannaCry.
- Outdated OpenSSL Version (CVE-2022-0778) - Medium Severity - CVSS: 7.5
  Description: Susceptible to DoS via certificate parsing issue.
- Unpatched Windows Services - High Severity - CVSS: 8.5
  Description: System is missing critical security patches.
- Weak SSH Cipher Suites - Medium Severity - CVSS: 6.5
  Description: Deprecated ciphers still enabled.
- RDP Port 3389 Exposed - Medium Severity - CVSS: 6.8
  Description: Brute-force attacks possible without firewall restrictions.

3. Critical Vulnerabilities:

1. SMBv1 Enabled

2. Unpatched Windows Services

3. Outdated OpenSSL Version

4. Recommended Fixes:

- Disable SMBv1 via Group Policy or Registry Editor.
- Install all pending Windows Updates immediately.
- Update OpenSSL to the latest stable version.
- Harden SSH configuration and disable deprecated ciphers.
- Restrict RDP access using firewall rules or VPN-only access.

5. Supporting Screenshots:

Screenshots included:

- Scan Setup
- Scan Progress
- Scan Result
- OpenVAS Web Interface Report

6. Summary:

This vulnerability assessment using OpenVAS against the Windows 10 target at 192.168.163.129 identified critical risks that require urgent remediation. Immediate steps include disabling outdated protocols, applying security patches, and tightening remote access controls.