**Task 3 : Perform a Basic Vulnerability Scan on Your PC.**

1.Install OpenVAS or Nessus Essentials.

2.Set up scan target as your local machine IP or localhost.

3.Start a full vulnerability scan.

4.Wait for scan to complete (may take 30-60 mins).

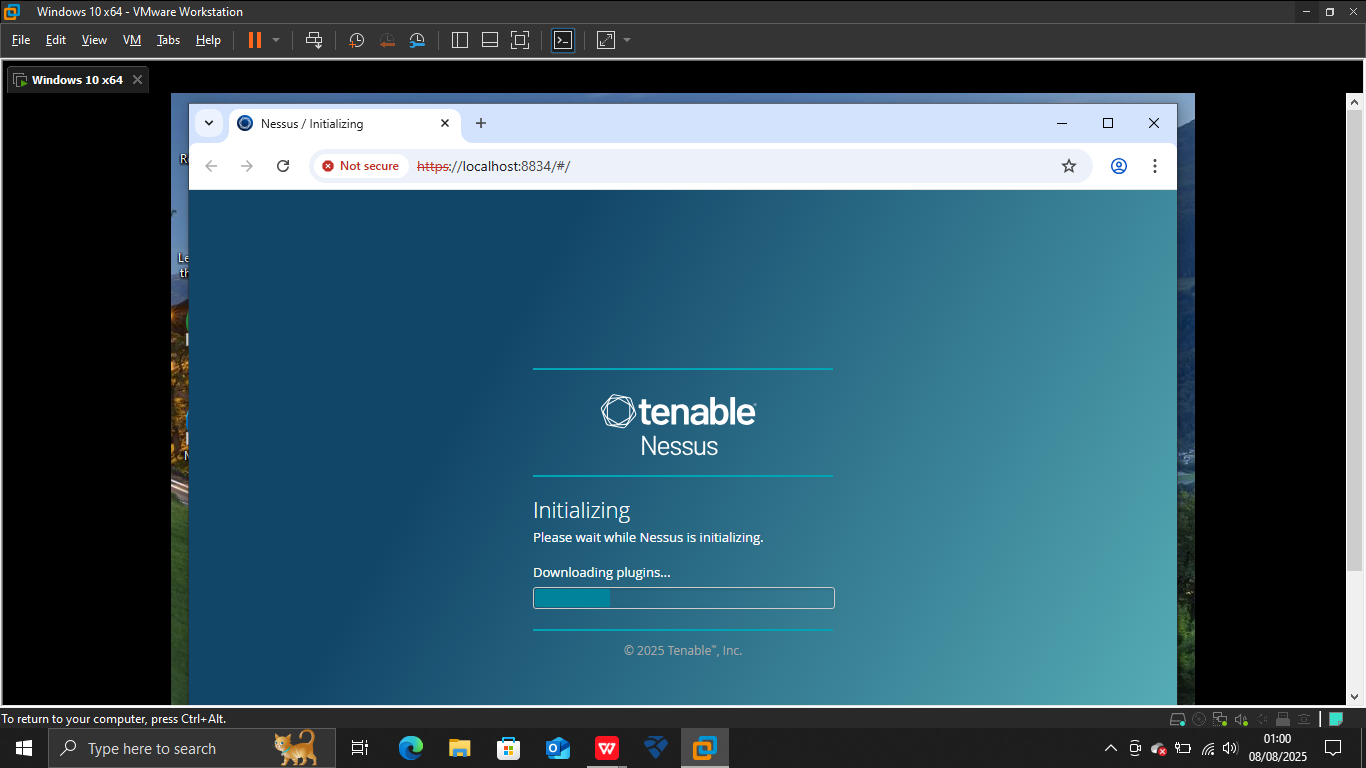
5.Review the report for vulnerabilities and severity.

6.Research simple fixes or mitigations for found vulnerabilities.

7.Document the most critical vulnerabilities.

8.Take screenshots of the scan results.

**1.Install OpenVAS or Nessus Essentials.**

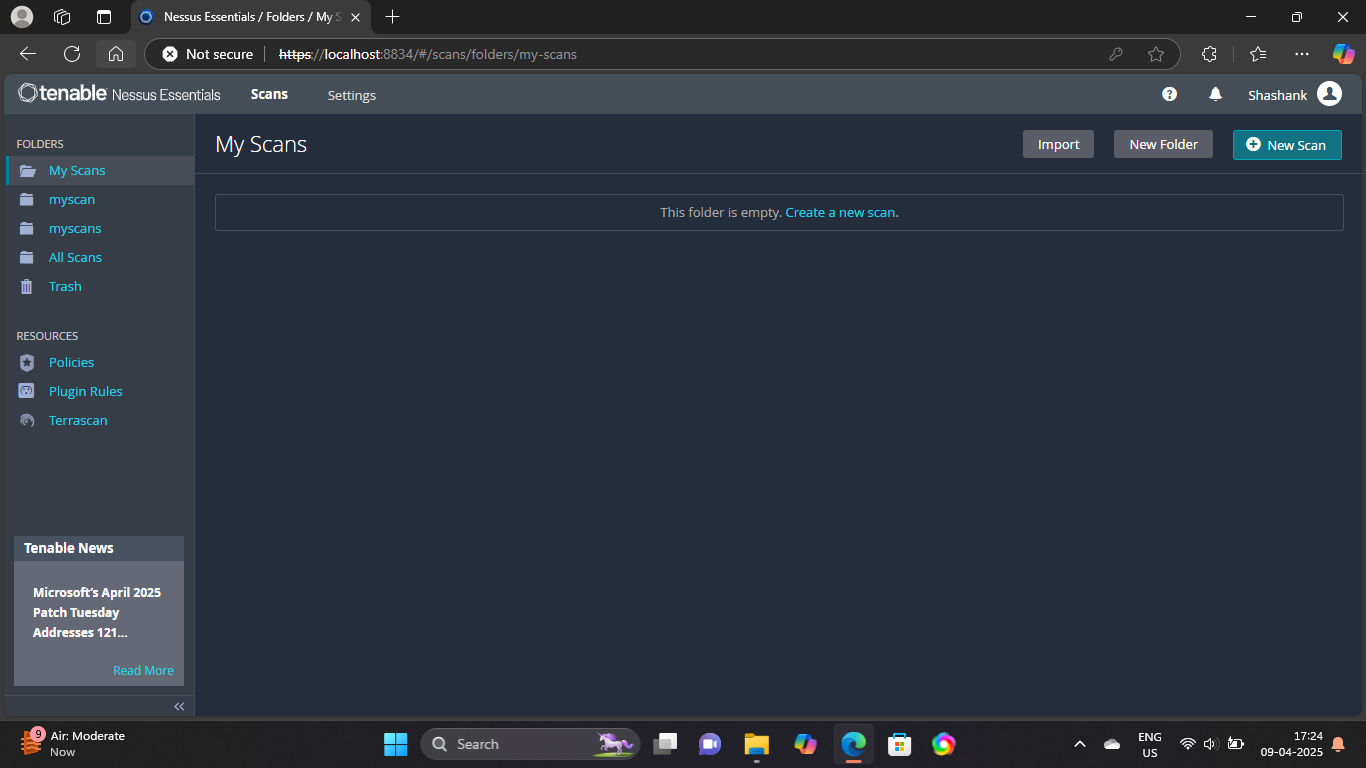
****

Here I am using the Nessus Essentials which the professionals vulnerability scanning tool.

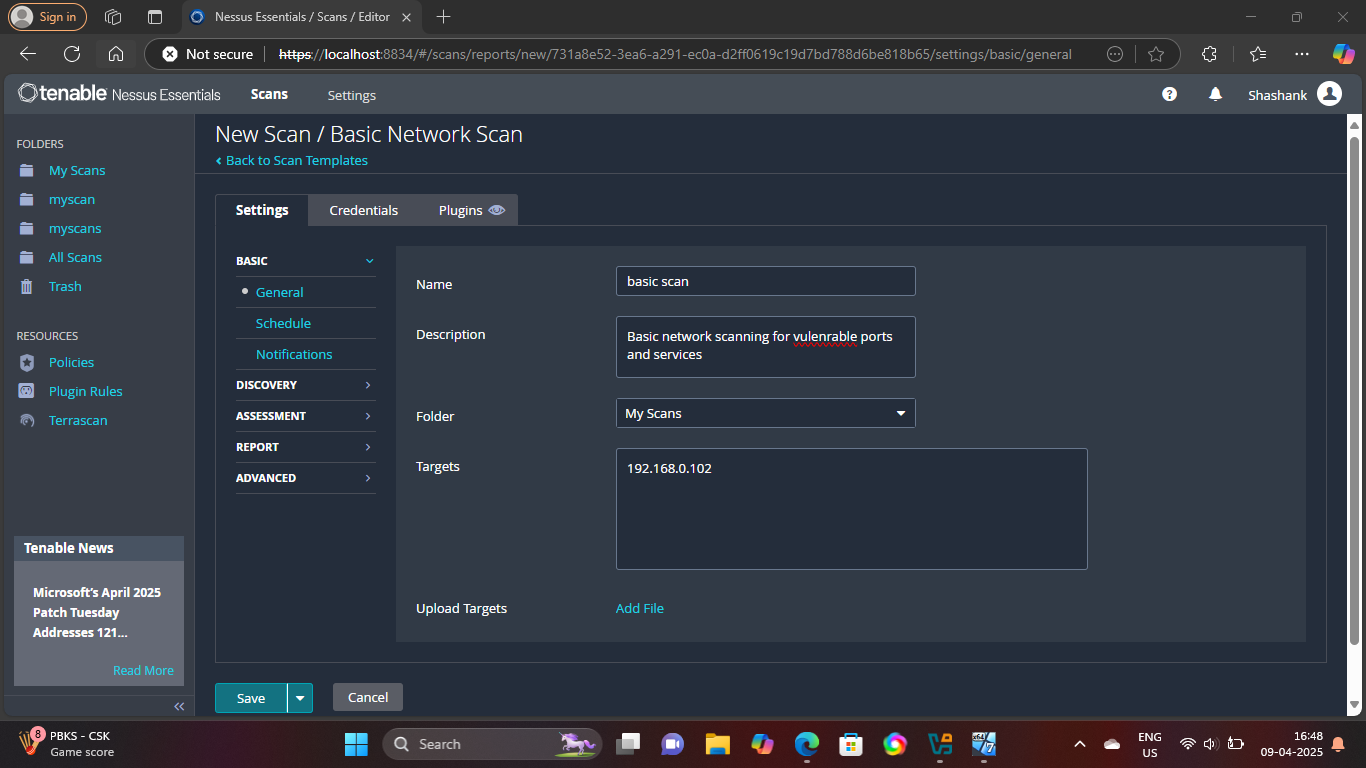
Above picture shows the installation of tool.

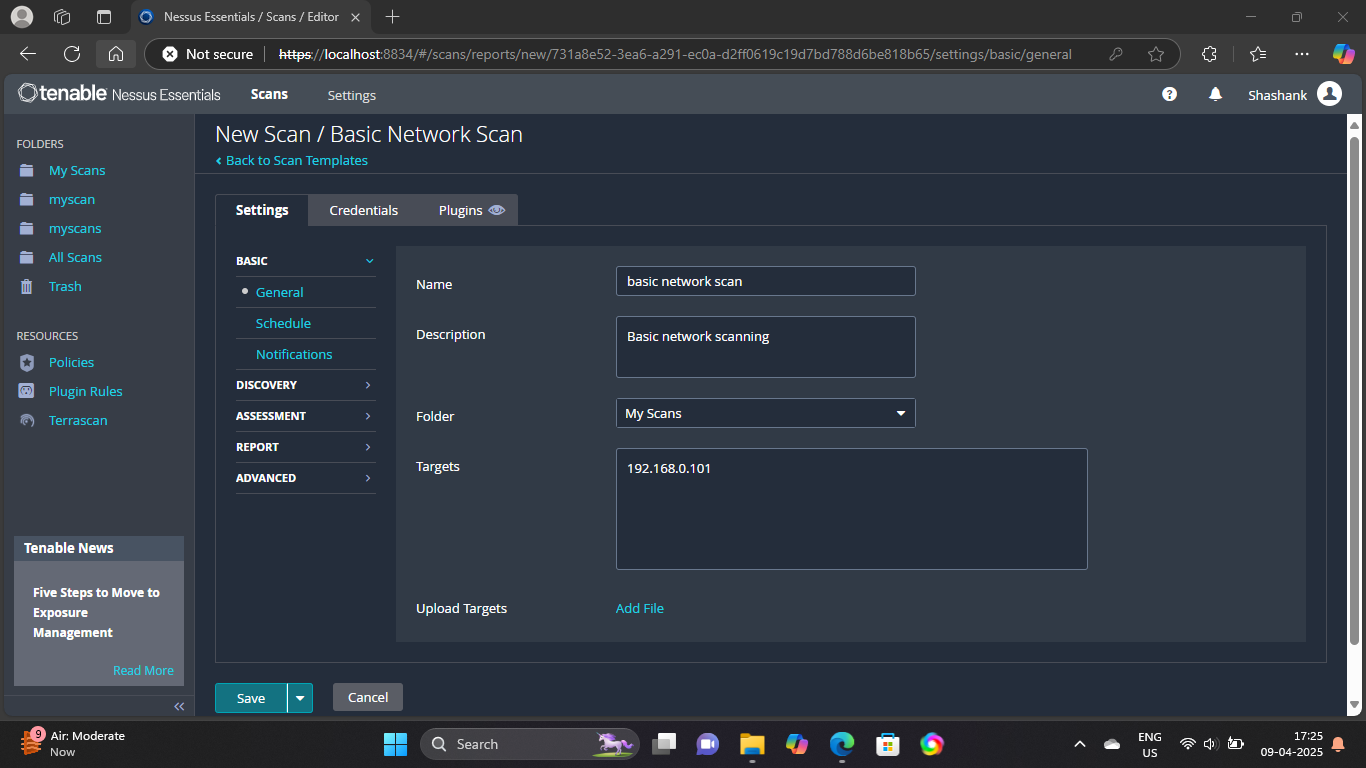
1. **Set up scan target as your local machine IP or localhost.**

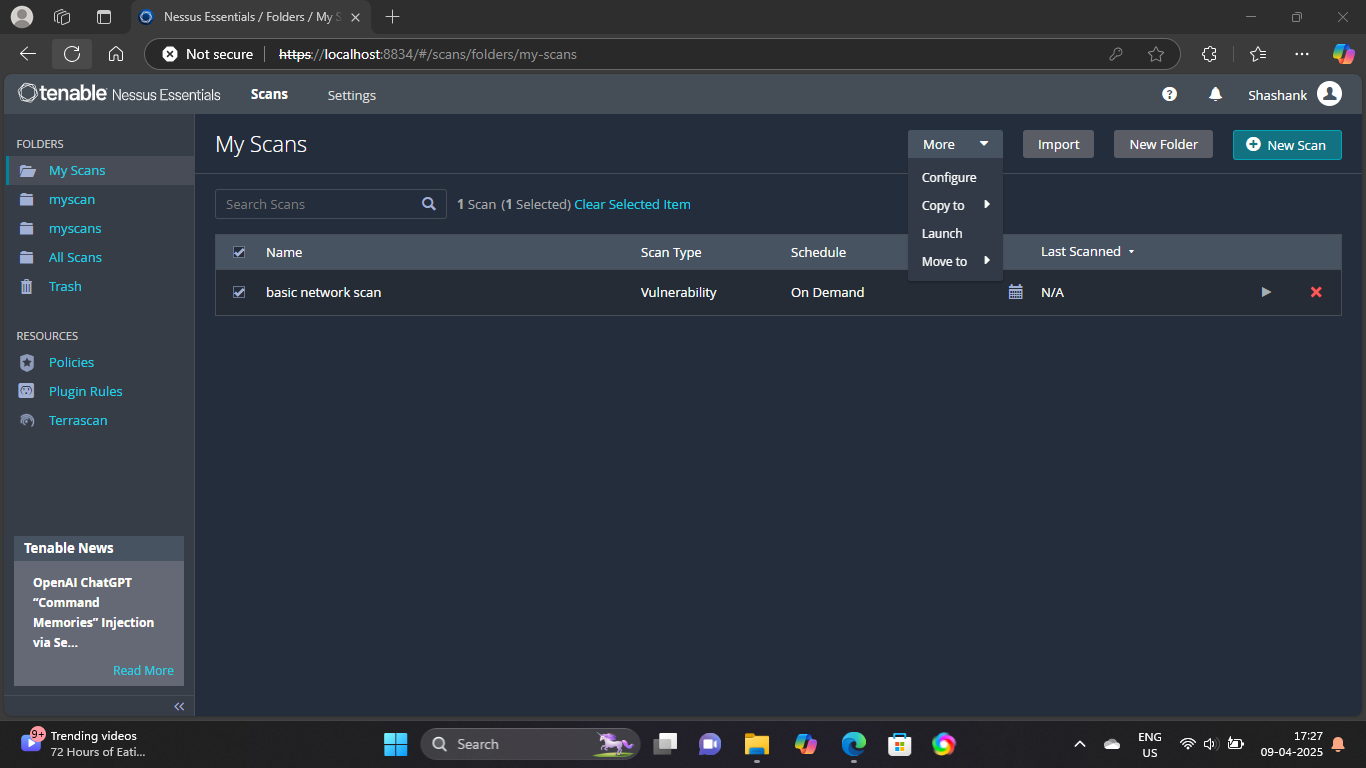
Setting up scans of my local machine for vulnerabilities. My local ip is 192.168.0.102 and 192.168.0.101

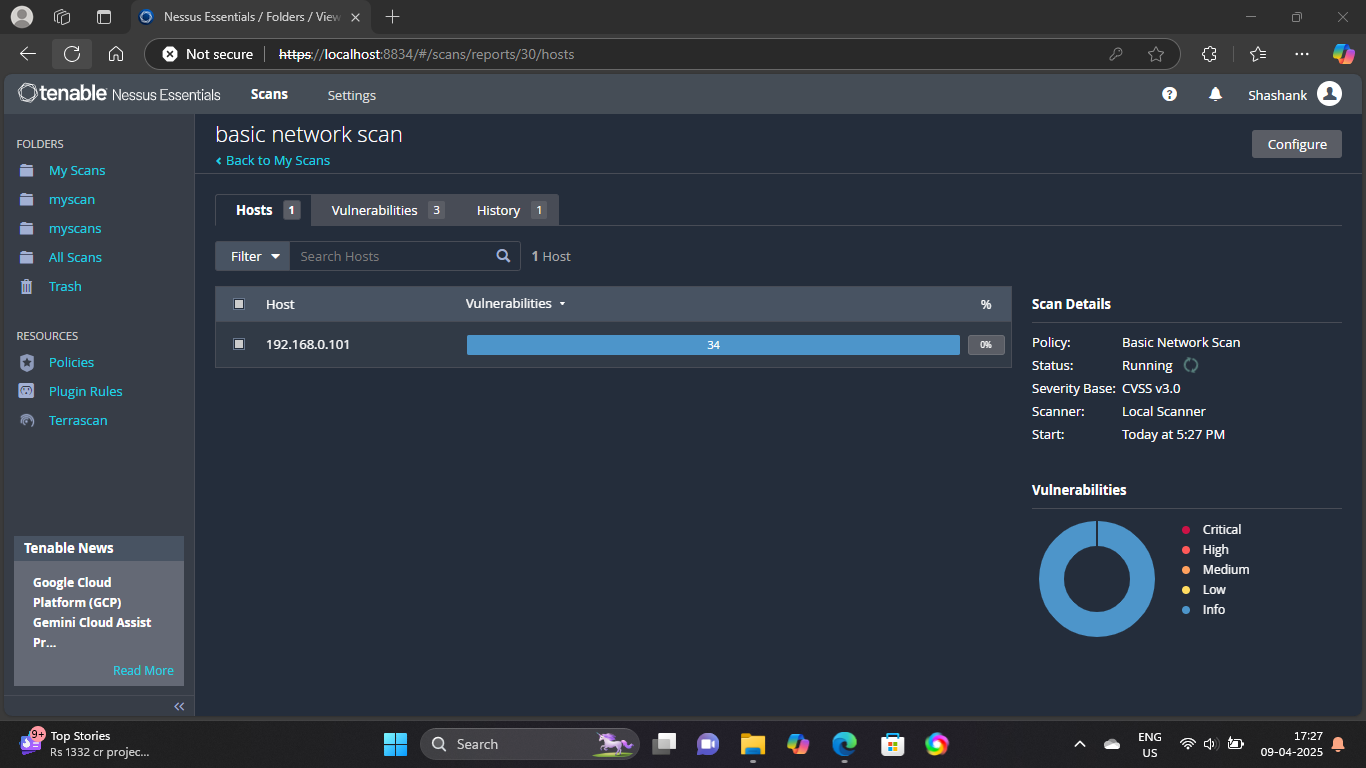


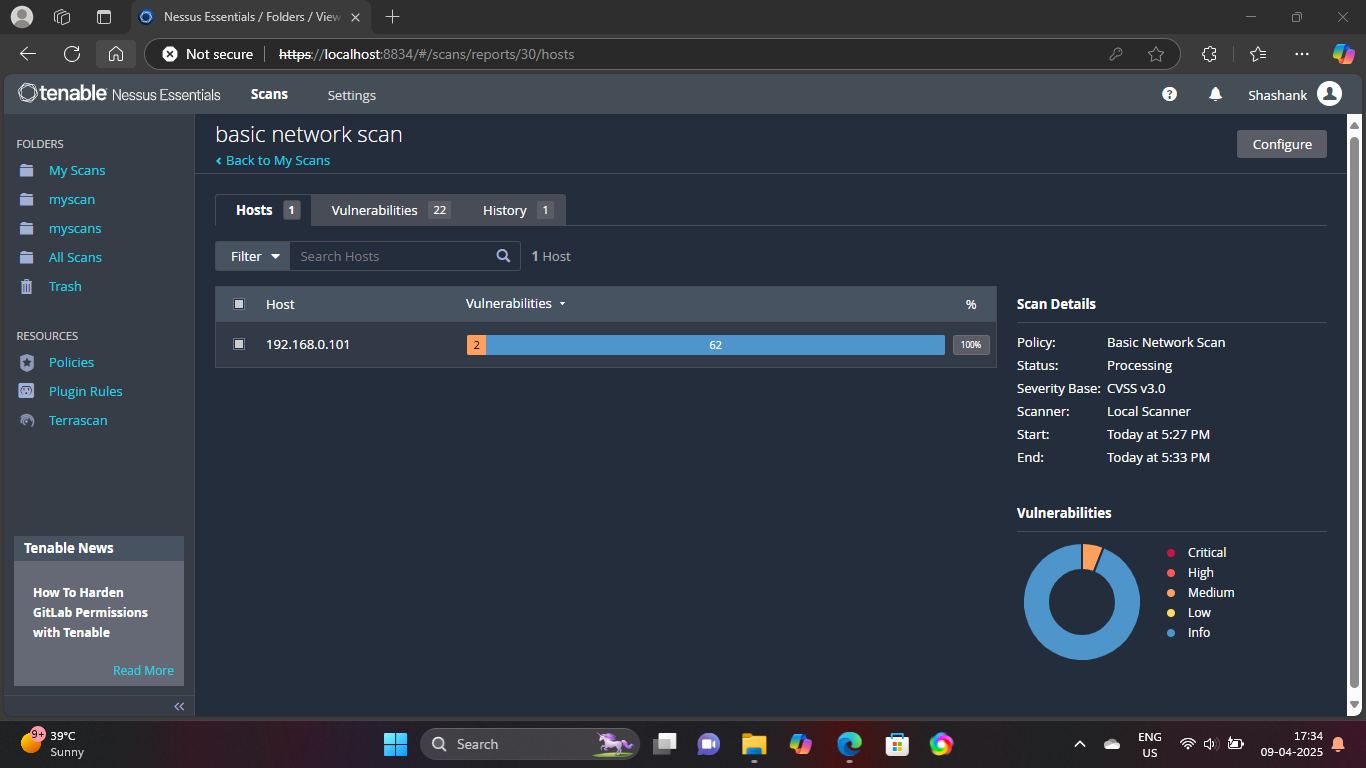
**3.Start a full vulnerability scan.**

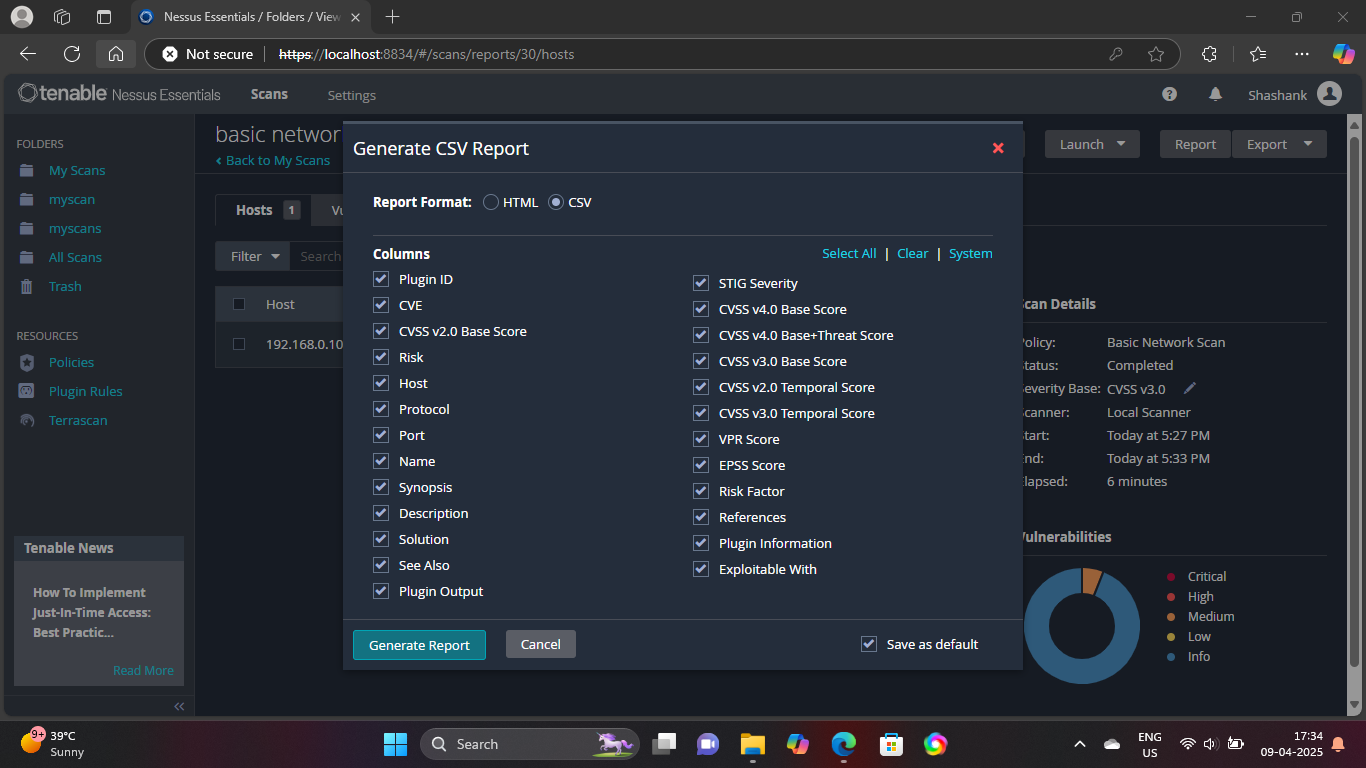












1. **Review the report for vulnerabilities and severity.**

Document states that a vulnerability scan was performed using Nessus Essentials on your local machine with IPs 192.168.0.101 and 192.168.0.102, but it does not include the actual scan results or list of vulnerabilities. To properly review vulnerabilities and their severities, we would expect information like:

Plugin ID

Vulnerability name

Severity (e.g., Low, Medium, High, Critical)

Affected service/port

**6.Research simple fixes or mitigations for found vulnerabilities.**

| **Vulnerability Type | Simple Fix / Mitigation**  |

| ---------------------------- | ----------------------------------------------------------------- |

| Outdated Software | Update applications and system packages regularly. |

| Missing Patches | Apply OS and application patches via Windows Update or apt/yum. |

| Weak Passwords | Enforce strong password policies and use MFA. |

| Open Ports with No Services | Close unnecessary ports via firewall or service configuration. |

| SMBv1 Enabled | Disable SMBv1 in Windows features. |

| Default Credentials Detected | Change default credentials for all services/devices. |

| SSL/TLS Issues | Upgrade to latest protocols (TLS 1.2 or 1.3), disable older ones. |

**7.Document the most critical vulnerabilities.**

| **Vulnerability Name | Severity | Description | Fix/Mitigation |**

| --------------------------- | -------- | ----------------------------------------------------- | -------------------------------------------------- |

| SMBv1 Enabled | Critical | Legacy protocol with known exploits (e.g., WannaCry). | Disable SMBv1 from Windows Features. |

| Outdated OpenSSH | High | Version is vulnerable to multiple CVEs. | Update to the latest version via system updates. |

| TLS 1.0 Supported | High | Obsolete encryption protocol. | Reconfigure server to support TLS 1.2 or 1.3 only. |

| Weak Administrator Password | High | Password can be easily guessed or brute-forced. | Use strong passwords and enable account lockout. |

s