Cyber Security Internship

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

**Objective:** Use free tools to identify common vulnerabilities on your computer.

**Tools:** OpenVAS Community Edition (free vulnerability scanner) or Nessus Essentials.

**Deliverables:** Vulnerability scan report with identified issues.

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

Installation of Nessus Essentials is done and username and password are created.

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

My localhost or local machine IP : “192.168.136.129” is given for Vulnerability scan.

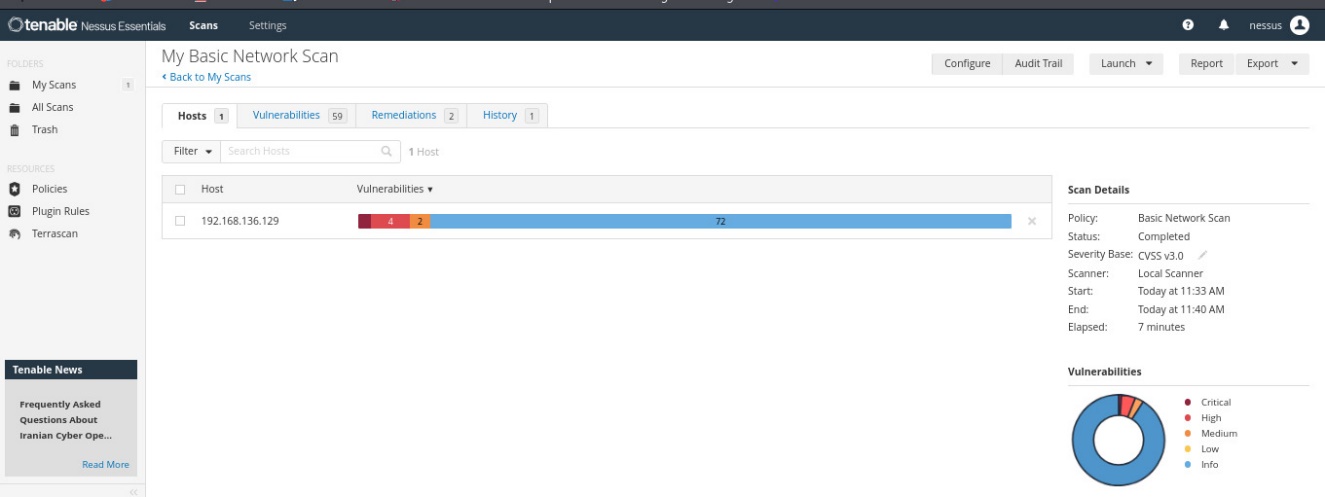
**3.Start a full vulnerability scan.**

Started the vunlnerability scan for mu local IP address   
 A screenshot of a computer

Description automatically generated

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

The Scan was done and shows the result as :



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

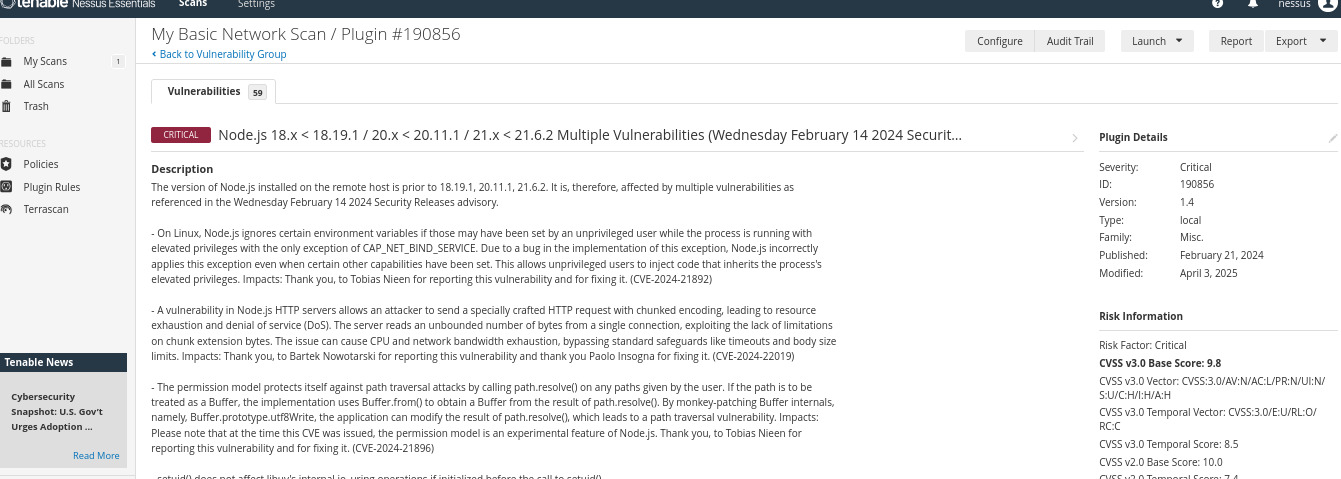
A screenshot of a computer

Description automatically generated

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

A screenshot of a computer

Description automatically generated



A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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

**Vulnerability 1:** Node.js 18.x < 18.19.1 / 20.x < 20.11.1 / 21.x < 21.6.2 Multiple Vulnerabilities

A vulnerability in Node.js HTTP servers allows an attacker to send a specially crafted HTTP request with chunked encoding, leading to **resource exhaustion and denial of service (DoS).**

**Severity:** Critical

**CVE:** CVE-2023-46809, CVE-2024-21890, CVE-2024-21891, CVE-2024-21892, CVE-2024-21896, CVE-2024-22017, CVE-2024-22019

**Fix:** Upgrade to Node.js version 18.19.1 / 20.11.1 / 21.6.2 or later.

**Vulnerability 2:** Python Library Tornado 6.5.0 DoS

**Severity:** High

**CVE:** CVE-2025-47287

**Fix:** Upgrade to Tornado version 6.5.0 or later.

**Vulnerability 3:** SSL Certificate Cannot Be Trusted

**Severity:** Medium

**Fix:** Purchase or generate a proper SSL certificate for this service.