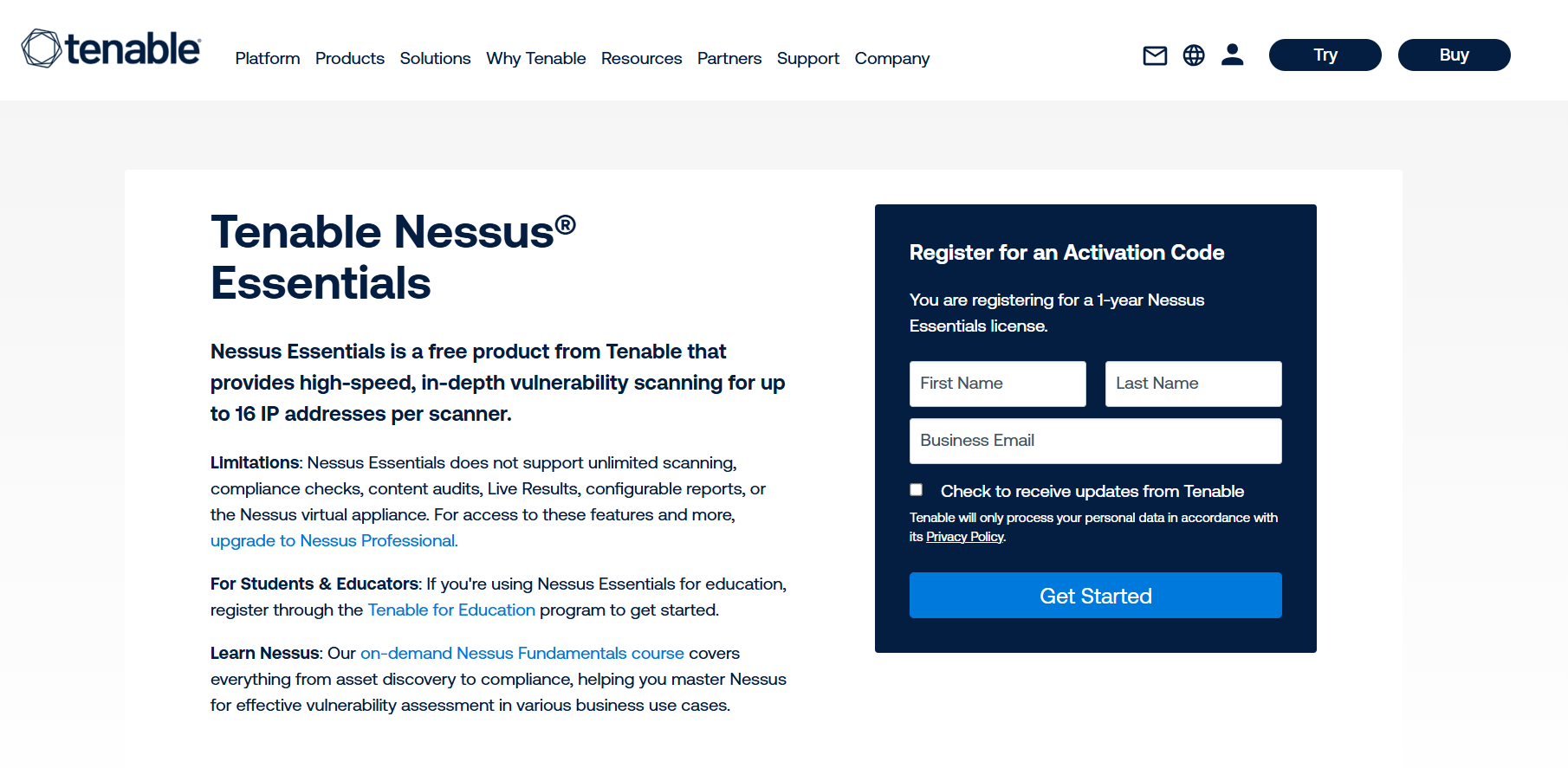
**TASK-3 Basic Vulnerability Scan on PC**

**Install Nessus Essentials**

1. Go to the official Tenable website - <https://www.tenable.com/products/nessus/nessus-essentials>
2. You'll need to provide your name and email address and click on Get Started



1. An email with an activation code will be sent to your email address. Save it for later.
2. Now, run the file as administrator.



1. After the installation process, your default web browser should automatically open to the Nessus web interface (usually <https://localhost:8834/>)
2. You may encounter a "Connection is not private" or "Security warning" because Nessus uses a self-signed SSL certificate initially. You'll need to bypass this warning (e.g., click "Advanced" then "Proceed to localhost" or "Accept the risk")
3. On the welcome screen, select "Nessus Essentials."
4. Enter the activation code you received via email.
5. Create an administrator account (username and password) for accessing the Nessus web interface
6. After setting up the admin account, Nessus will begin downloading and compiling its plugins. (Time consuming process)

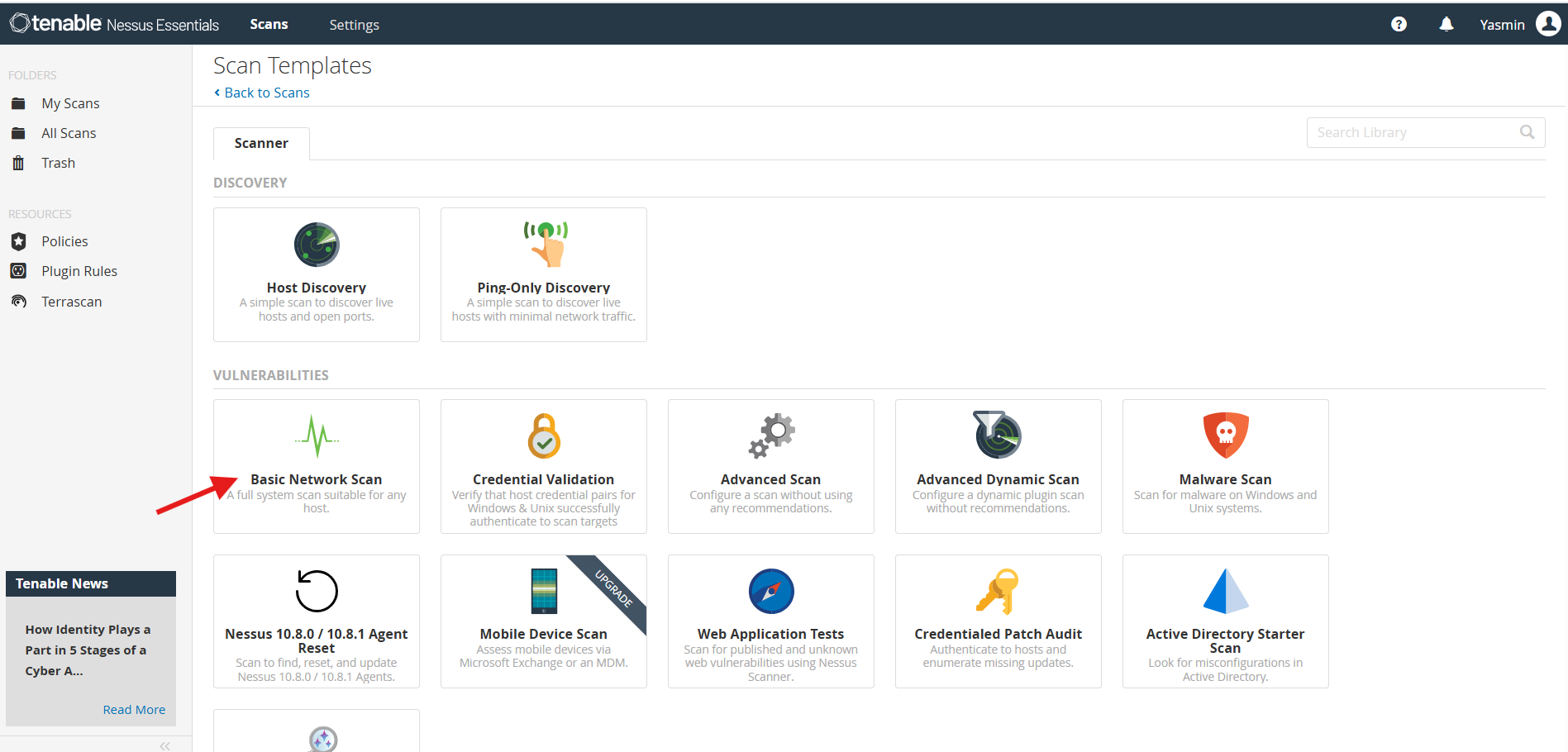
**Full Scan**

Now Click on the New Scan button

A screen shot of a computer

AI-generated content may be incorrect.

Click on the Basic Network Scan for a Full system scan

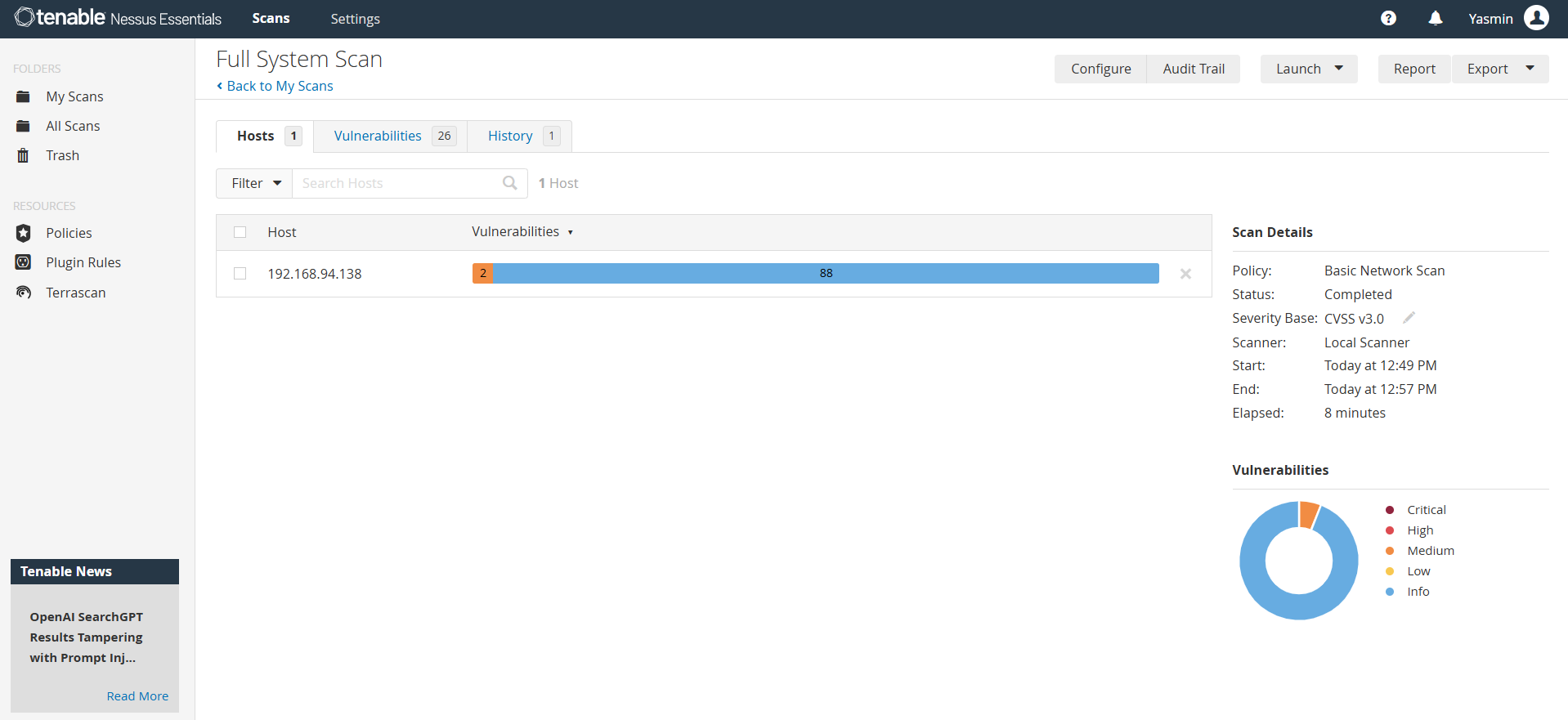


Give the target to scan and wait some time for the scan to be completed.

**Results of the Scan (Detailed scan report attached in HTML file)**

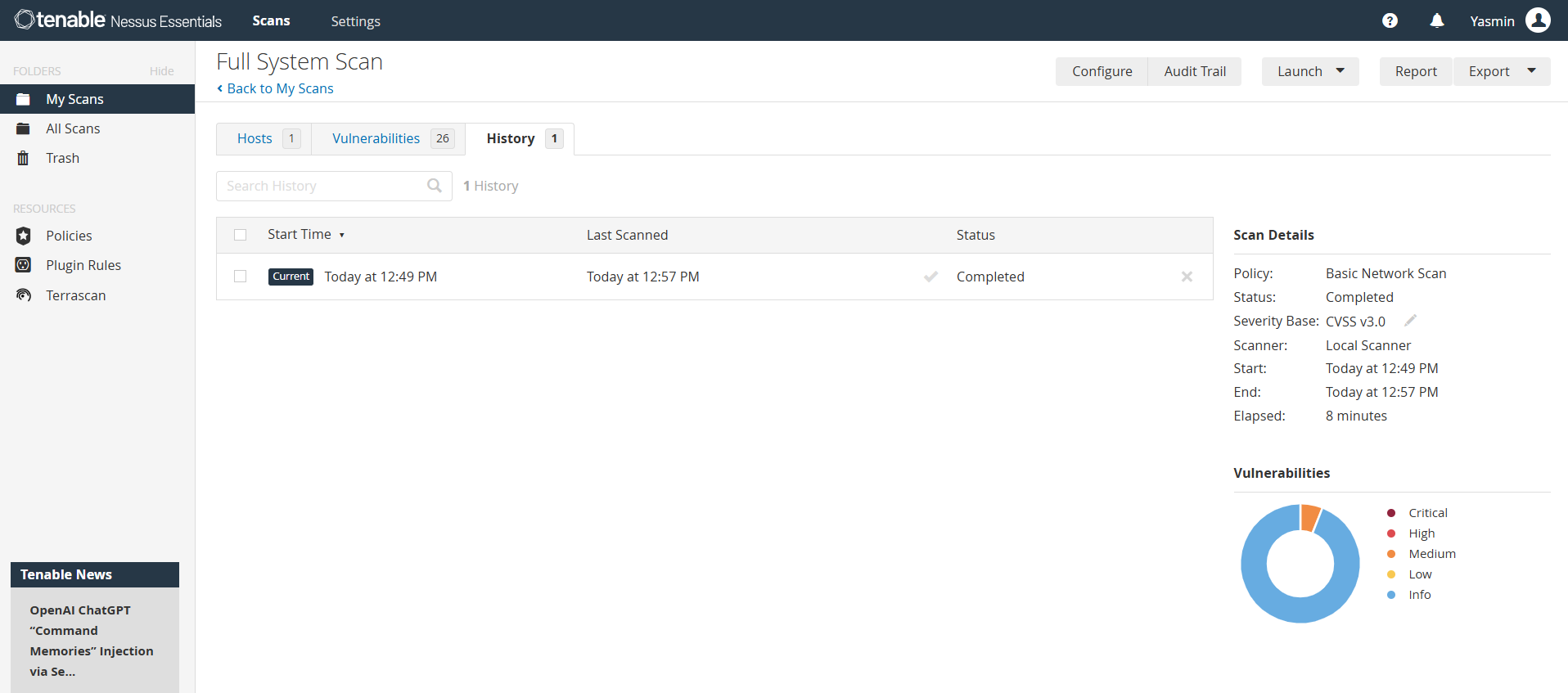
Only 2 vulnerabilities were found, and they are medium. Remaining 88 were informational, not a vulnerability but provides information about the target.

Below are the images of the result of the scan

****

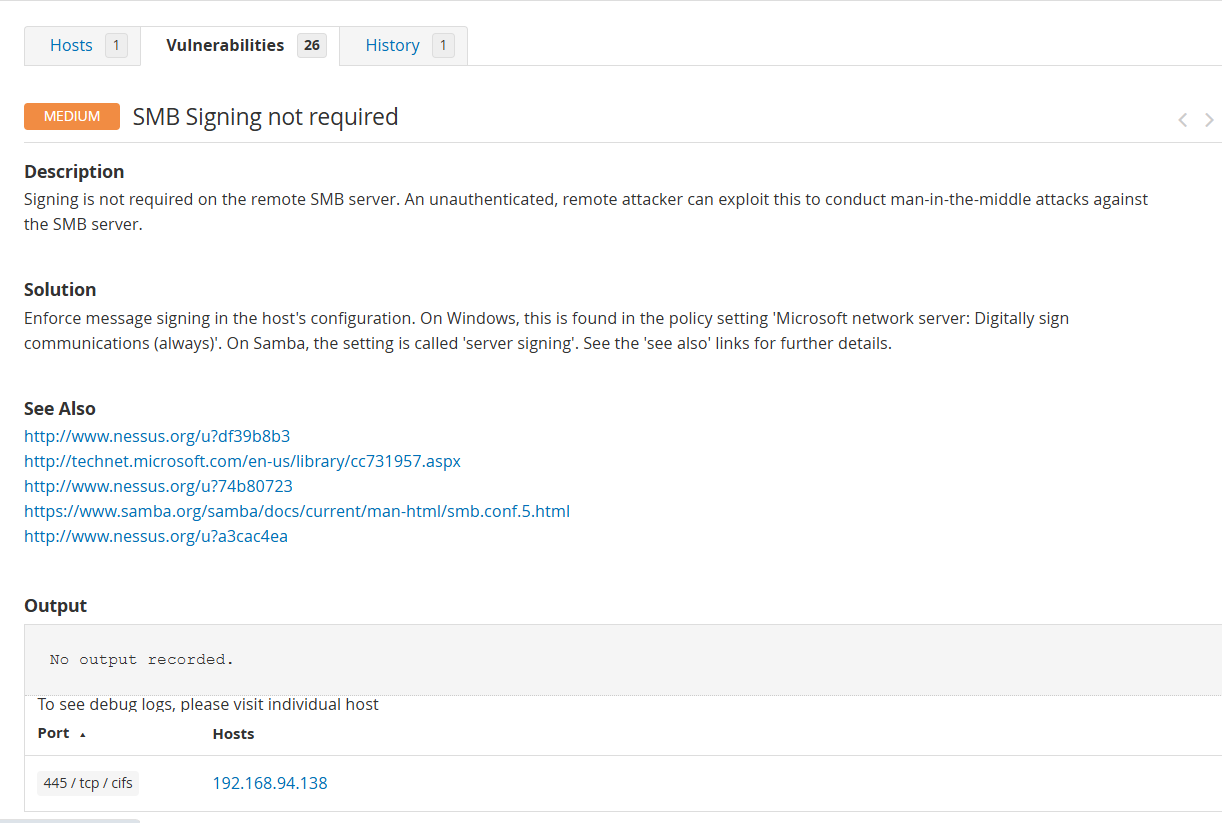
**A screenshot of a computer

AI-generated content may be incorrect.**

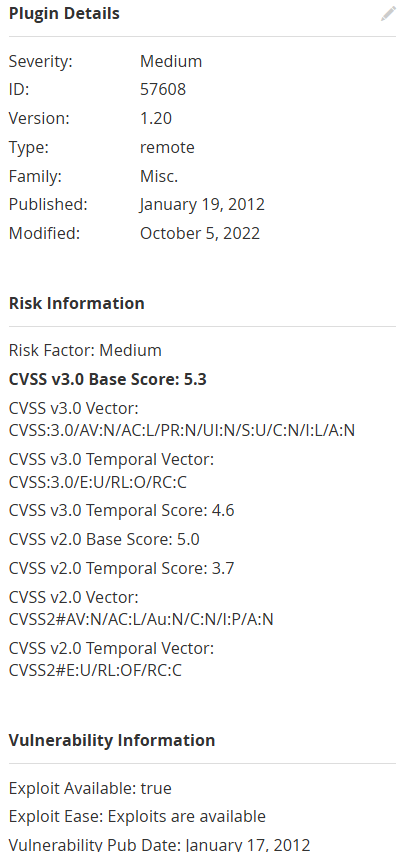
****

**Description and Mitigation**

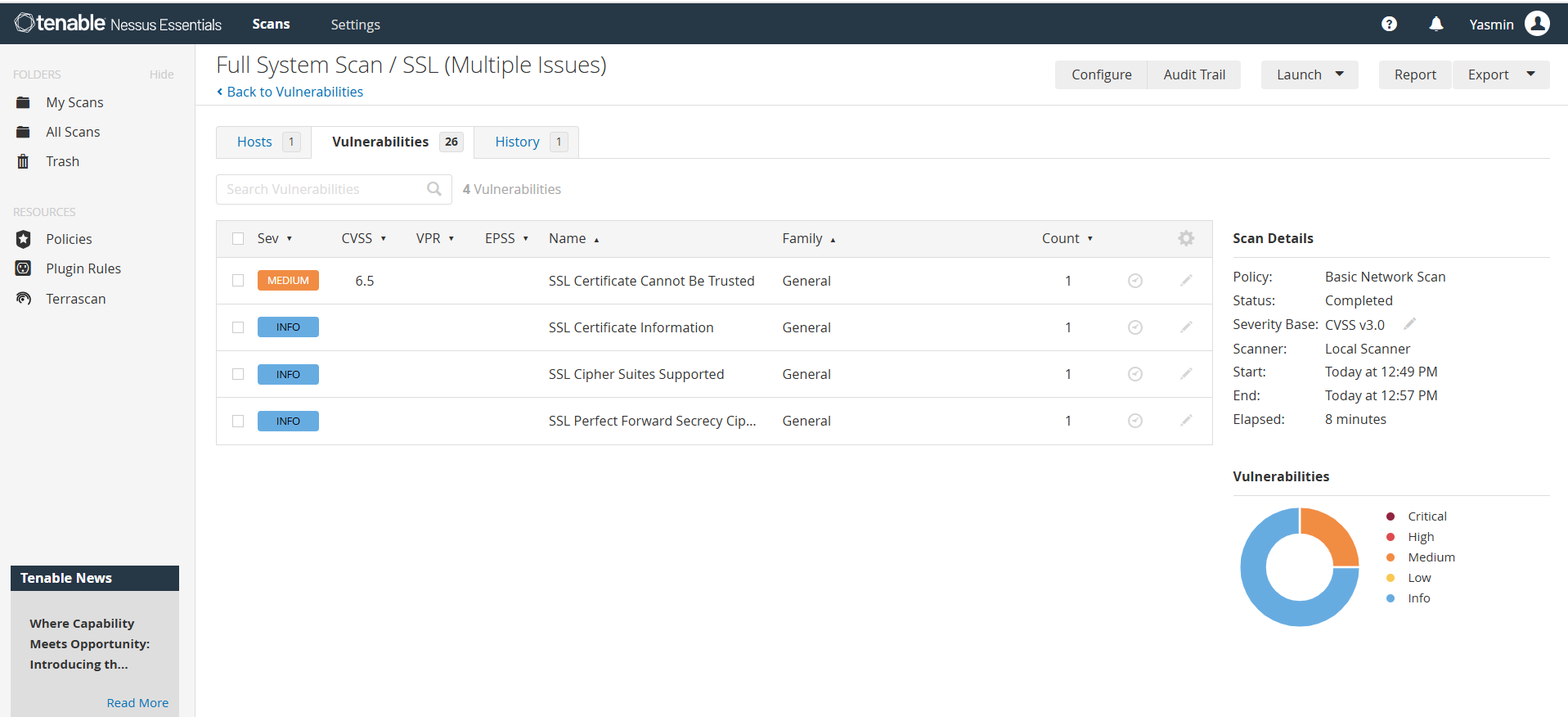
1. First medium vulnerability description and solution along with the IP address and hosts affected by this vulnerability is included in the vulnerabilities tab



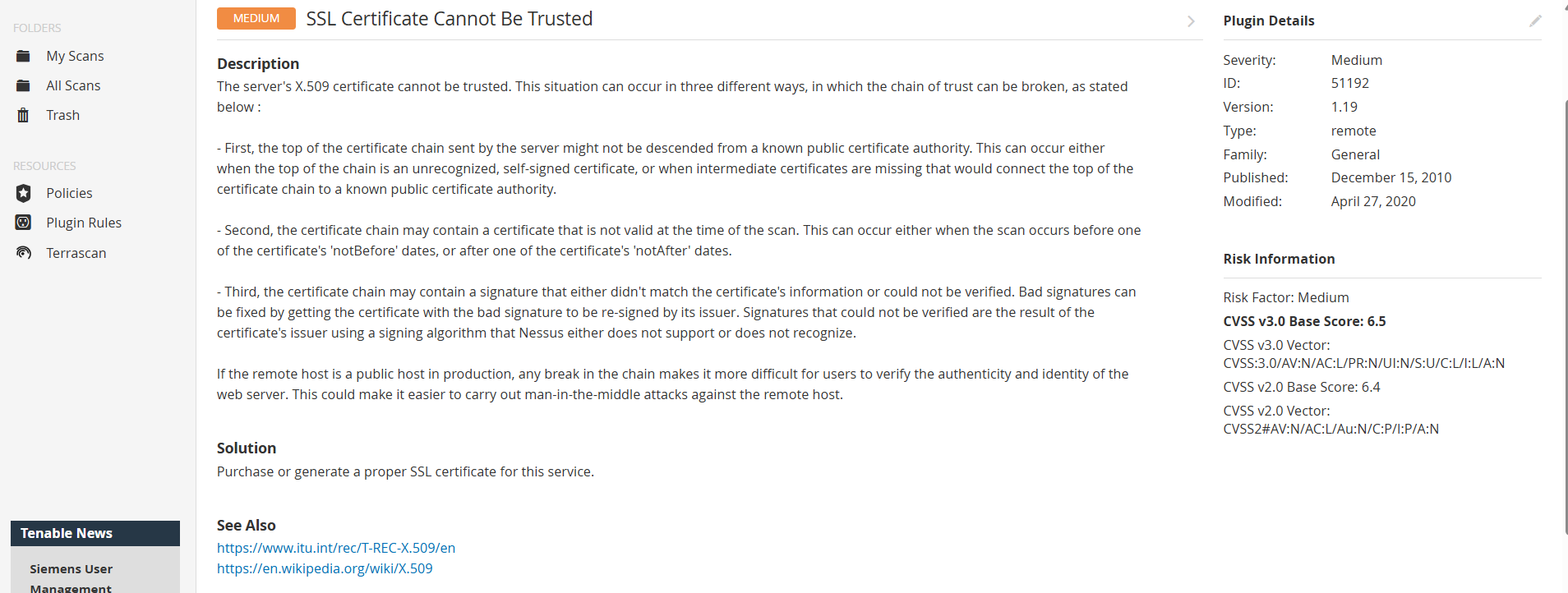
The plugin details of the first medium vulnerability



1. Second vulnerability is mixed consisting both medium and informational vulnerabilities.



The medium vulnerability description and solution along with the IP address and hosts affected by this vulnerability is included in the vulnerabilities tab. The plugin details are also included.



A close-up of a message

AI-generated content may be incorrect.