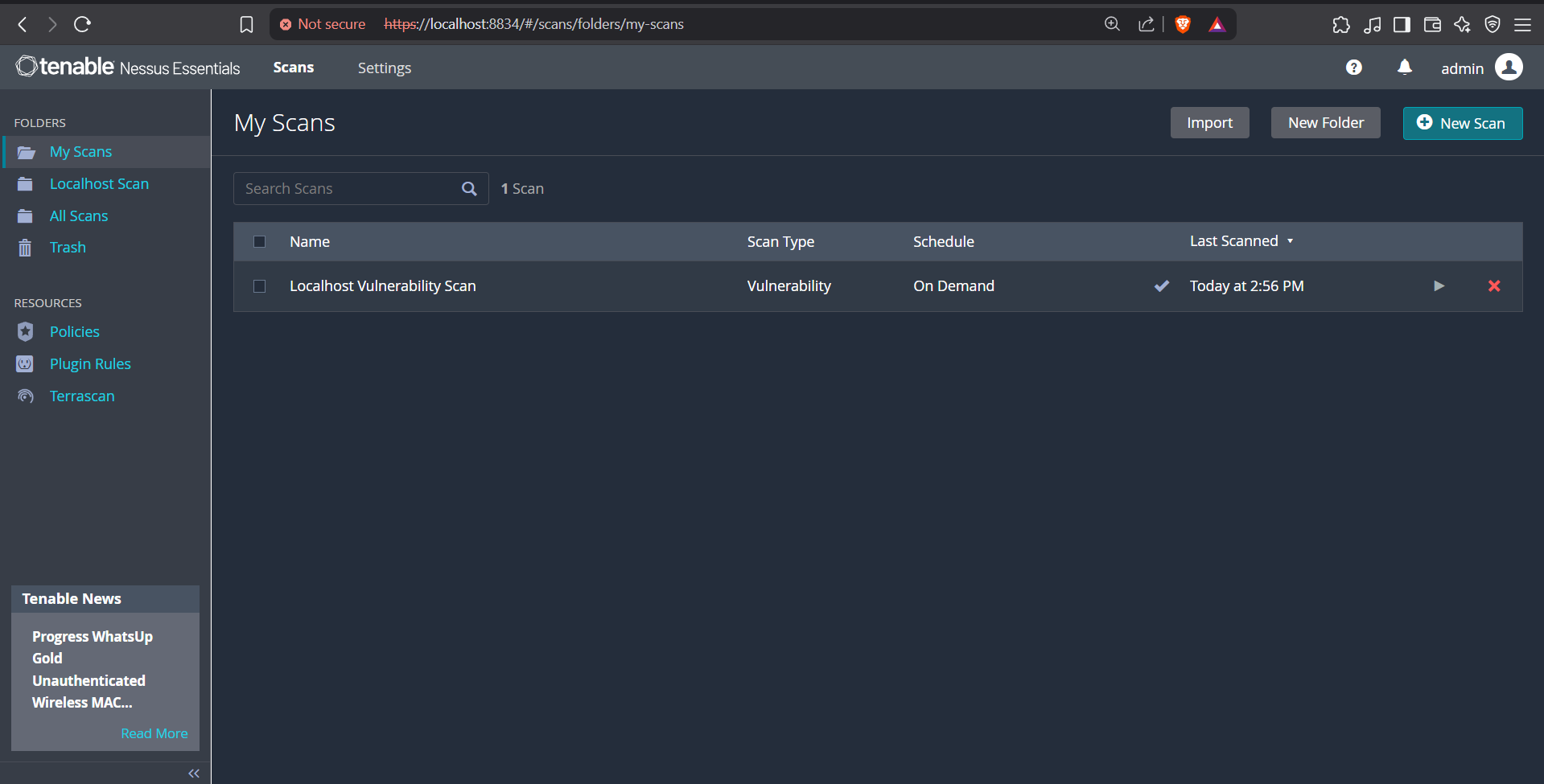
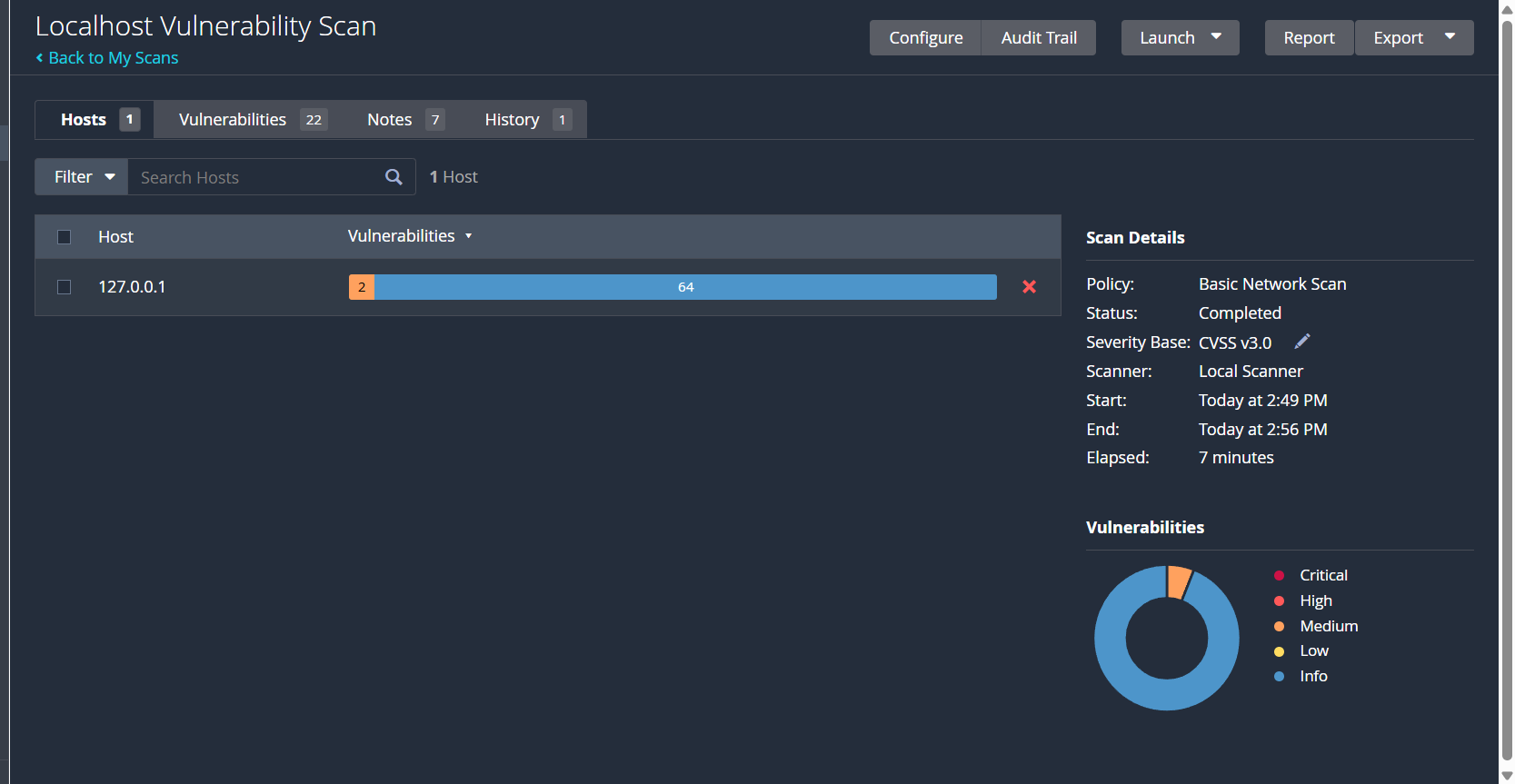
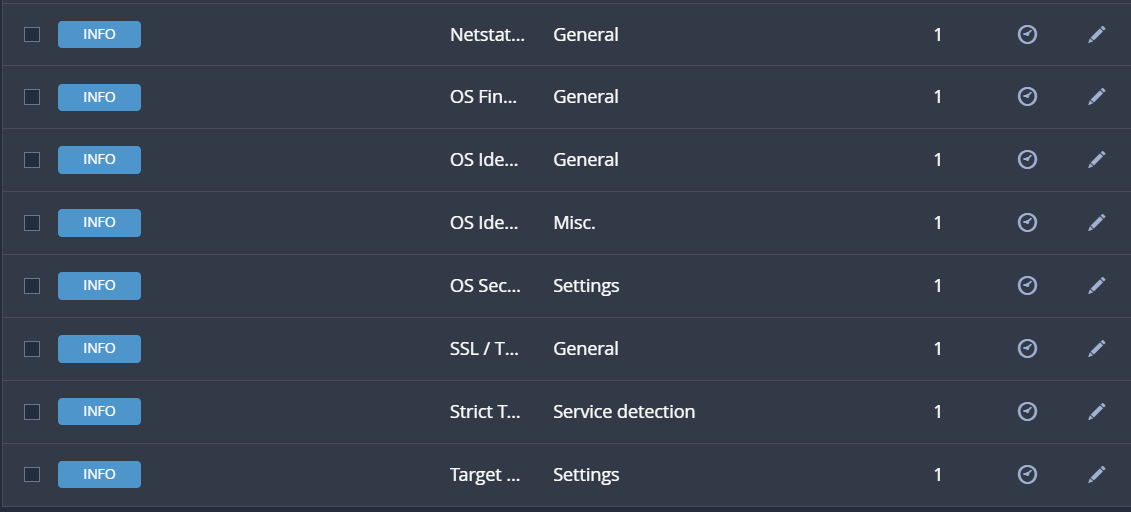
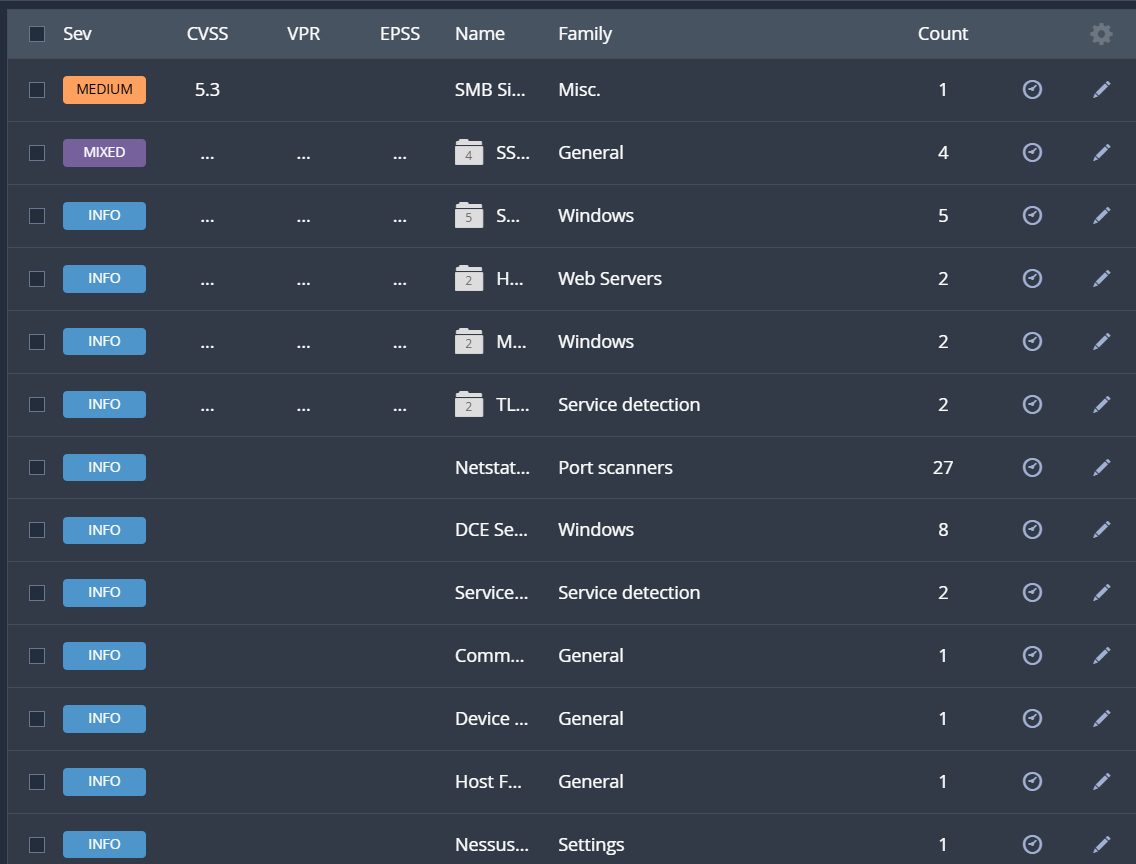
SCAN:







SCAN RESULT

|  |  |
| --- | --- |
| **Severity Level** | **Number of Vulnerabilities** |
| **Critical** | 0 |
| **High** | 0 |
| **Medium** | 1 |
| **Low** | 0 |
| **Mixed** | 1 |
| **Informational** | 20 |
| **Total** | **22** |

MEDIUM LEVEL Vulnerability:

**Plugin Name:** SMB Signing not required

**Severity:** Medium

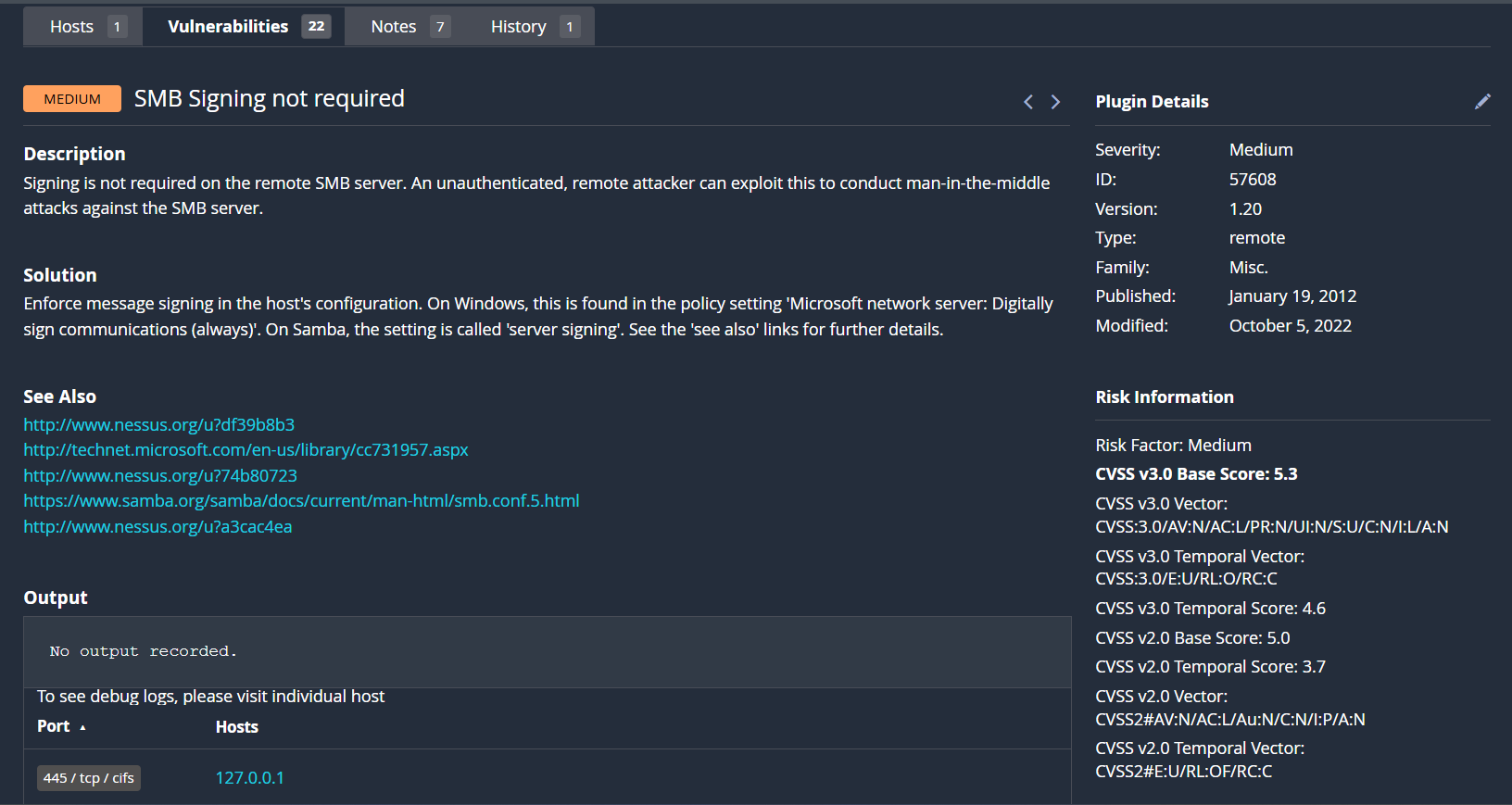
**Port:** 445/tcp (CIFS)

**Host:** 127.0.0.1

**Description:** The SMB (Server Message Block) server running on your local machine does not require SMB message signing. This means that an attacker on the same network could potentially carry out man-in-the-middle (MITM) attacks, intercepting or modifying traffic between the SMB client and server.

**Solution:**

* Go to Local Security Policy > Local Policies > Security Options.
* Enable "Microsoft network server: Digitally sign communications (always)".



MIXED LEVEL Vulnerability:

**Plugin Name:** SSL Certificate Cannot Be Trusted

**Severity:** Medium

**Port:** 8834/tcp (www)

**Host:** 127.0.0.1

**Description:** The X.509 certificate used by the server cannot be trusted. This trust issue arises due to one or more of the following reasons:

* Unrecognized Certificate Authority (CA):

The certificate chain may end with a self-signed certificate or is missing intermediate certificates connecting it to a trusted public CA.

* Certificate Validity Period Issue:

The certificate may be expired or not yet valid at the time of scanning.

* Unverifiable or Invalid Signature:

The certificate may contain a bad or unverifiable signature, potentially signed using an algorithm not supported or recognized by Nessus.

If this certificate is being used in a production environment, these issues can hinder users from verifying the identity of the server and open the door to MITM (man-in-the-middle) attacks.

**Solution:**

* Use a certificate signed by a trusted CA.
* Ensure the certificate is within its validity period.
* Check that all intermediate certificates are properly configured.
* If self-signed for local testing, no action may be necessary—but avoid using self-signed certs in public/production-facing services.

