**🛡️ Basic Vulnerability Scan Report**

**Tool Used**: Nessus Essentials  
**Scan Date**:01/06/2025  
**Scan Target**: 192.168.56.1  
**Scan Duration**: 23 mins

1. **Executive Summary:**

| **Severity** | **Number of Vulnerabilities** |
| --- | --- |
| Critical | 0 |
| High | 0 |
| Medium | 1 |
| Mixed | 1 |
| Info | 24 |

1. **Top Critical Vulnerabilities:**

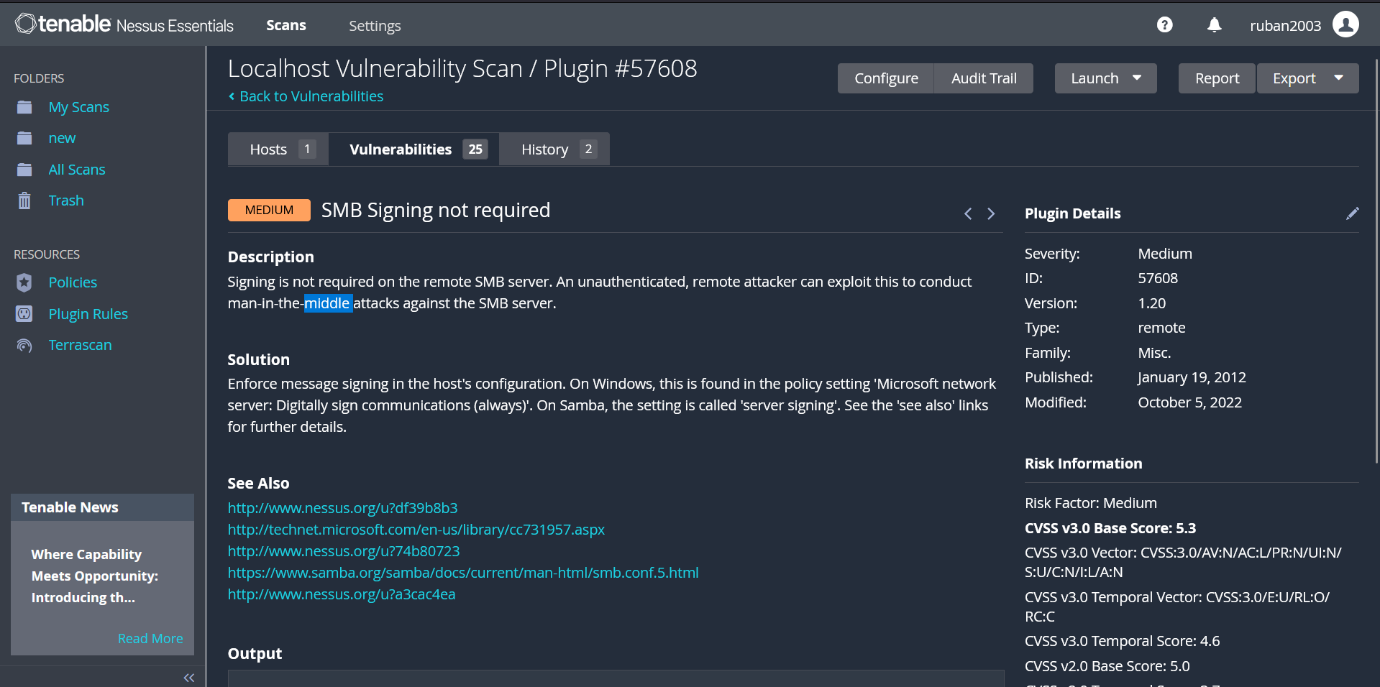
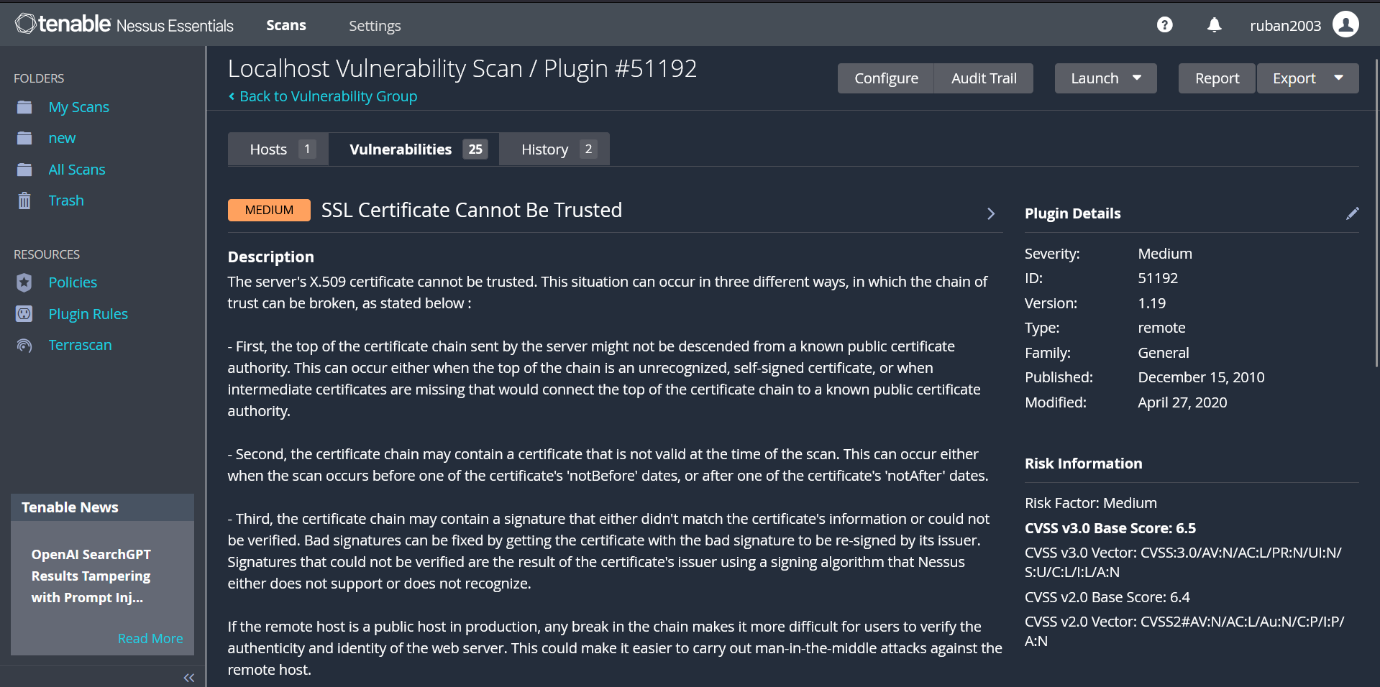
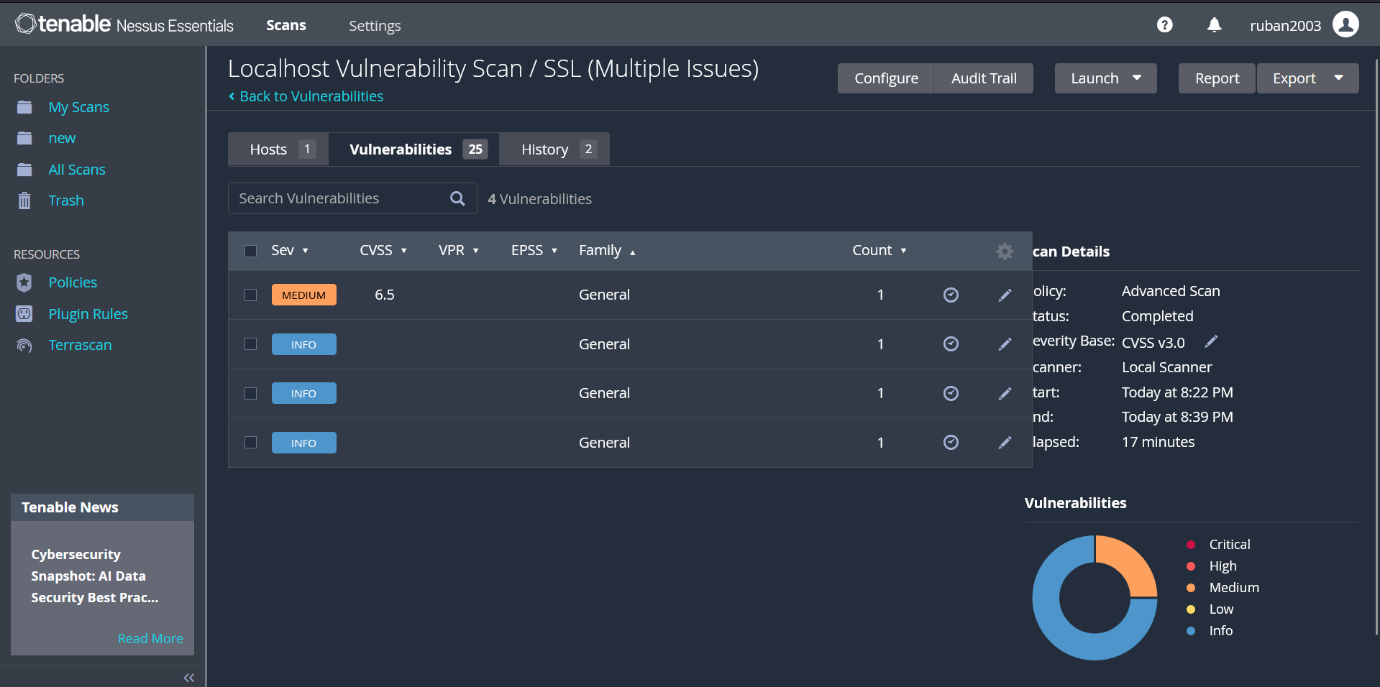
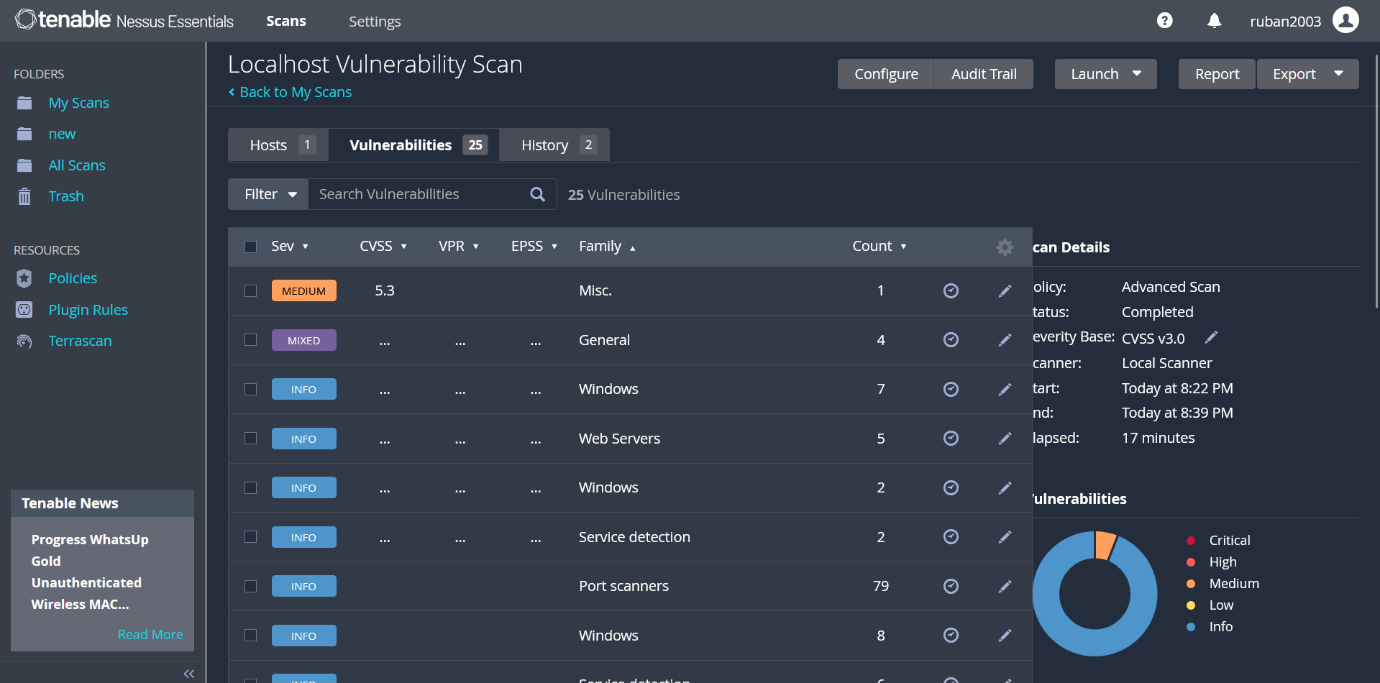
**1. Vulnerability 1: SMB Signing not required:**

* **Severity**: Medium
* **CVE ID**: 57608
* **Description**: Signing is not required on the remote SMB server. An unauthenticated, remote attacker can exploit this to conduct man-in-the-middle attacks against the SMB server.
* **Impact**: **Man-in-the-Middle, Steal sensitive data, tamper with SMB packets**
* **Solution**: Enforce message signing in the host's configuration. On Windows, this is found in the policy setting 'Microsoft network server: Digitally sign communications (always)'. On Samba, the setting is called 'server signing'. See the 'see also' links for further details.
* **Affected Port**: 445 / tcp / cifs

**2.Vulnerability 2:SSL Certificate Cannot Be Trusted:**

* **Severity**: Medium
* **CVE ID**: 51192
* **Description**: The server's X.509 certificate cannot be trusted. This situation can occur in three different ways, in which the chain of trust can be broken, as stated below :  
    
  - First, the top of the certificate chain sent by the server might not be descended from a known public certificate authority. This can occur either when the top of the chain is an unrecognized, self-signed certificate, or when intermediate certificates are missing that would connect the top of the certificate chain to a known public certificate authority.  
    
  - Second, the certificate chain may contain a certificate that is not valid at the time of the scan. This can occur either when the scan occurs before one of the certificate's 'notBefore' dates, or after one of the certificate's 'notAfter' dates.  
    
  - Third, the certificate chain may contain a signature that either didn't match the certificate's information or could not be verified. Bad signatures can be fixed by getting the certificate with the bad signature to be re-signed by its issuer. Signatures that could not be verified are the result of the certificate's issuer using a signing algorithm that Nessus either does not support or does not recognize.  
    
  If the remote host is a public host in production, any break in the chain makes it more difficult for users to verify the authenticity and identity of the web server. This could make it easier to carry out man-in-the-middle attacks against the remote host.
* **Impact:**Lack of Trust, Susceptibility to MITM Attacks
* **Solution**: Purchase or generate a proper SSL certificate for this service.
* **Affected Port**: 8834 / tcp / www

**3.Screenshots:**

****

**4.Conclusion:**

The vulnerability scan performed on the target system 192.168.56.1 using Nessus Essentials identified no critical or high-severity vulnerabilities, which indicates a generally secure system configuration. However, two medium-severity vulnerabilities were discovered that could pose security risks if left unaddressed:

1. SMB Signing Not Required (CVE-57608): This leaves the system vulnerable to Man-in-the-Middle (MITM) attacks, allowing potential attackers on the network to intercept or tamper with SMB communications. Enforcing SMB signing is recommended to ensure message integrity.
2. Untrusted SSL Certificate (CVE-51192): The server is using an SSL certificate that cannot be verified due to issues with the certificate chain. This may lead to MITM attacks and erodes user trust. A valid certificate from a recognized Certificate Authority should be installed.