# **Vulnerability Assessment with Nessus Essentials**

## **Summary**

In this project, I used Nessus Essentials, a powerful vulnerability scanning tool, to assess my local network's security. The objective was to identify potential vulnerabilities, analyze the findings, and recommend remediation strategies to strengthen the network's security posture.

This project demonstrates my ability to:

* Set up and execute network scans.
* Interpret scan results to identify vulnerabilities.
* Provide actionable insights to mitigate security risks.

Below is a step-by-step breakdown of the process, along with key insights at each stage.

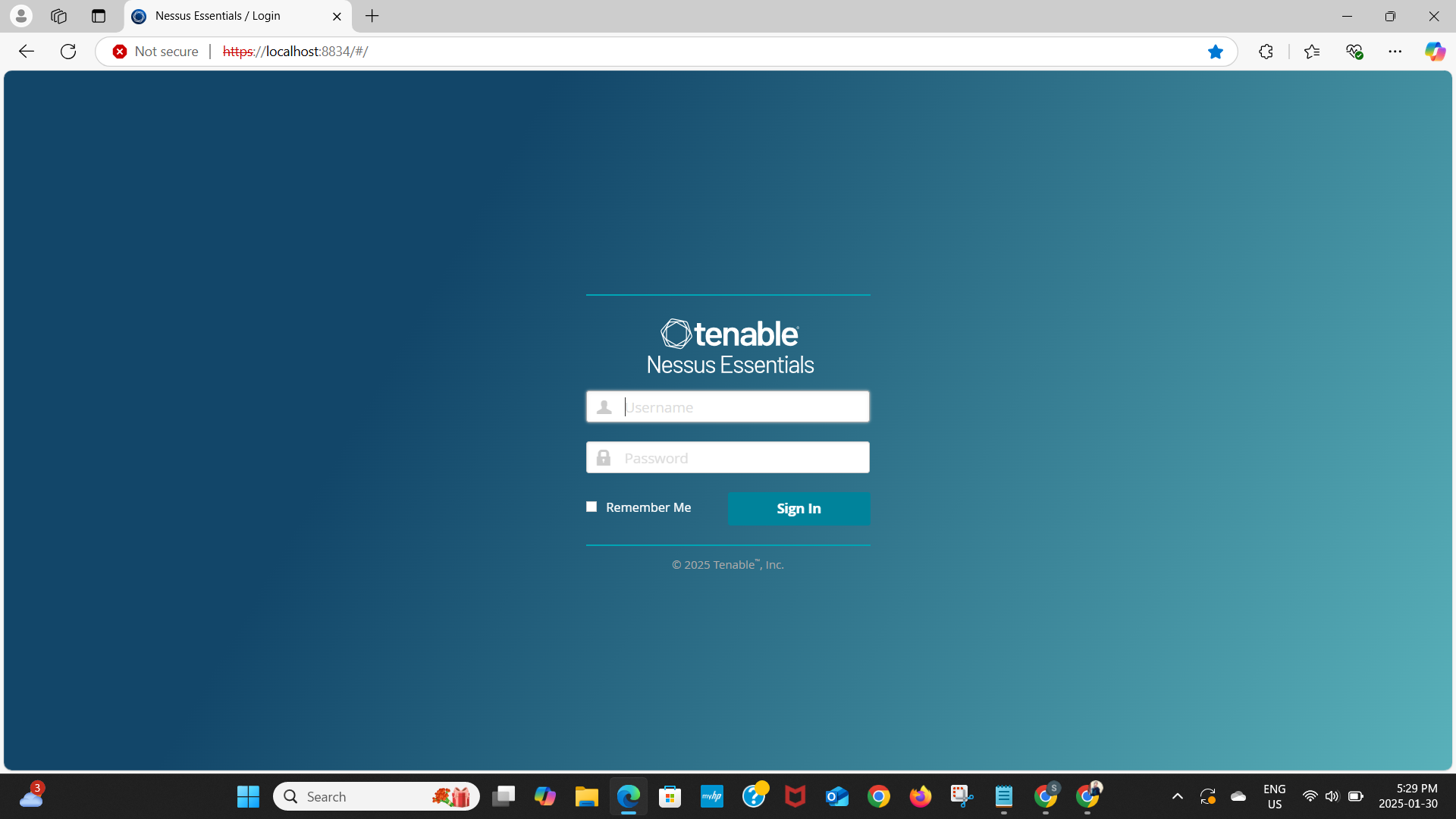
## **Phase 1: Setting Up Nessus Essentials**

### **Description**

The first step involved installing and configuring Nessus Essentials. The tool provides a user-friendly interface with various scan templates and configuration options.

### **Key Notes**

* Nessus Essentials is a free version suitable for small-scale environments.
* It includes powerful features such as plugin updates and comprehensive vulnerability detection.
* Proper setup ensured I was ready to run effective scans.
* Login to tenable Nessus Essentials



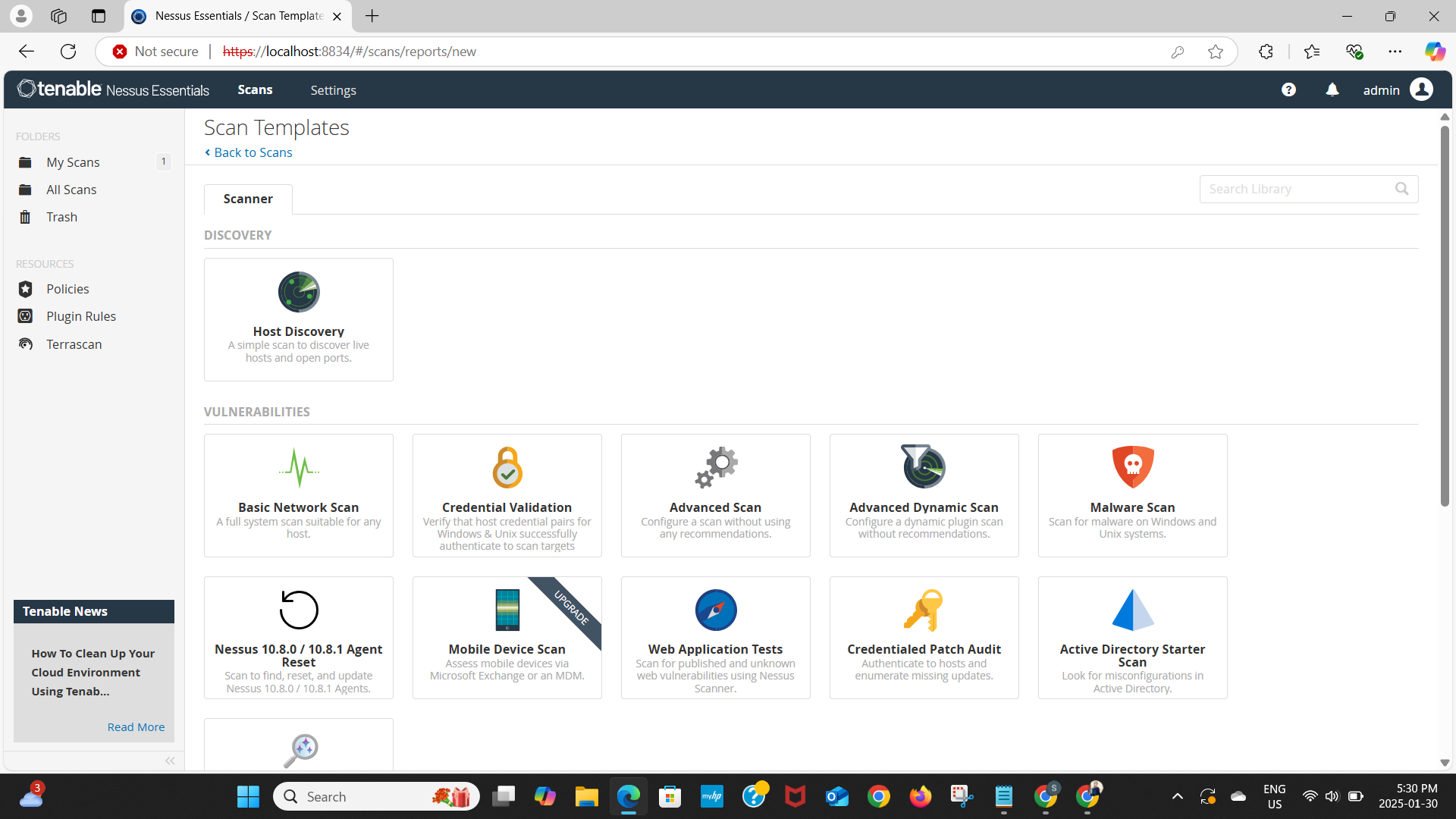
## **Phase 2: Choosing a Scan Template**

### **Description**

For this assessment, I selected the **Basic Network Scan** template, which is ideal for detecting vulnerabilities across multiple devices within a network.

### **Key Notes**

* This template identifies software misconfigurations, outdated patches, and other security gaps.
* Scan targets can include specific IP addresses or an entire range.



## **Phase 3: Configuring the Scan**

### **Description**

I configured the scan to cover my home network using the **192.168.1.0/24** subnet, ensuring all connected devices were assessed.

### **Key Notes**

* The scan was assigned a descriptive name and targeted all relevant IPs.
* Default plugin settings were used to maximize the scope of vulnerability detection.

## **Phase 4: Launching the Scan**

### **Description**

Once configured, I launched the scan from the Nessus dashboard. The tool began identifying vulnerabilities across the specified IP range.

### **Key Notes**

* Real-time progress updates were available during the scan.
* The duration varied depending on network size and device count.

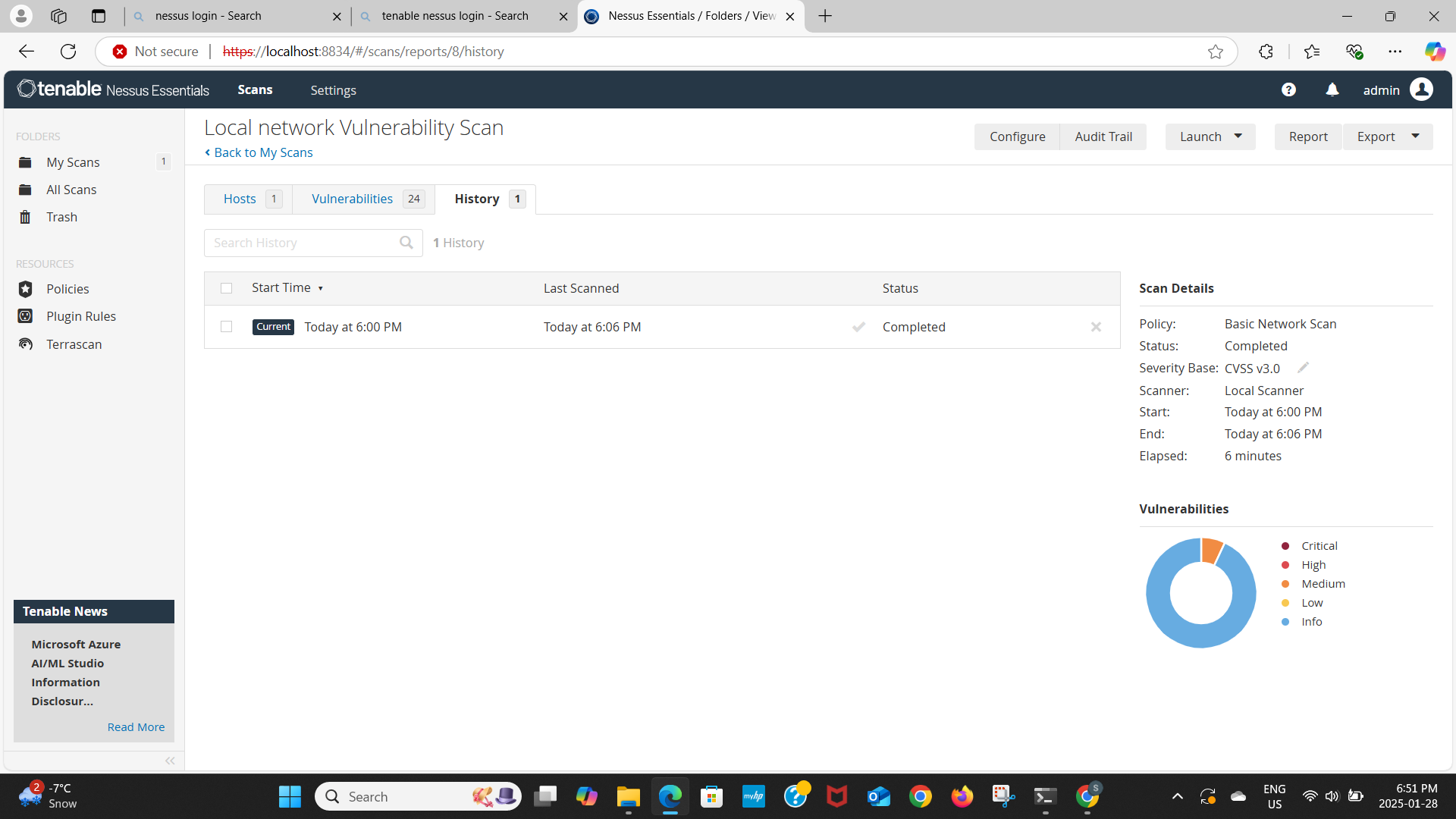
## **Phase 5: Reviewing the Scan Results**

### **Description**

The scan results provided a detailed report of detected vulnerabilities, categorized by severity: **Critical, High, Medium, and Low.**

**Key Notes**

* The most severe vulnerabilities were prioritized for remediation.
* Each finding included a description, affected systems, and recommended fixes.



## **Phase 6: Analyzing Critical Vulnerabilities**

### **Description**

I focused on analyzing **critical vulnerabilities**, reviewing key details such as:

* Vulnerability name
* Affected system and IP
* Plugin details
* Recommended remediation steps

### **Key Notes**

* Understanding the root cause of vulnerabilities is crucial for effective mitigation.
* Addressing these issues helps prevent threats such as **unauthorized access and data breaches**.

## **Phase 7: Report on Critical Vulnerabilities**

### **Introduction**

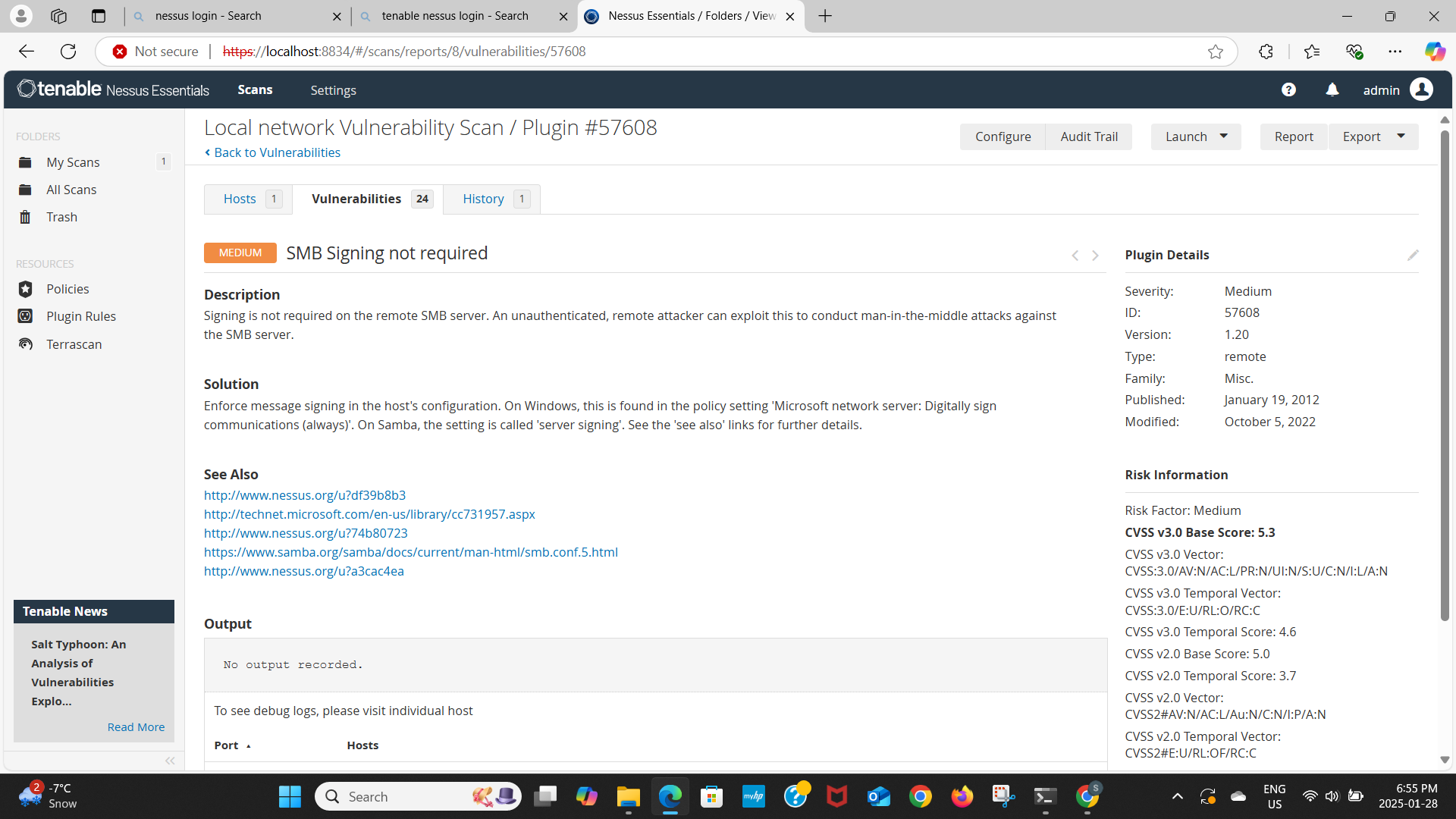
This report summarizes the most critical vulnerabilities identified during the Nessus scan, including their impact, potential risks, and recommended mitigation strategies.

### **Critical Vulnerabilities Overview**

There are 24 vulnerabilities. I found only two vulnerabilities with medium severity.

**Host: 192.168.55.1**

* **Vulnerability:** SMB Signing Not Required
* **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:** Unauthorized access to sensitive files and potential system compromise.
* **Remediation:** Configure the server to require SMB signing.



**Host: 192.168.55.1**

* **Vulnerability:** SSL Self-Signed Certificate
* **Description:** The X.509 certificate chain for this service is not signed by a recognized certificate authority. If the remote host is a public host in production, this nullifies the use of SSL as anyone could establish a man-in-the-middle attack against the remote host.
* **Impact:** Unauthorized access to sensitive files and potential system compromise. Without a trusted certificate, encrypted communication cannot be guaranteed to be secure.
* **Remediation:** Replace the self-signed certificate with a trusted SSL/TLS certificate.

## **Analysis and Insights**

### **Common Themes**

Many vulnerabilities were related to outdated configurations, weak encryption, and insecure protocols. This underscores the importance of **regular audits and patch management**.

### **Potential Risks**

Unresolved vulnerabilities expose the network to **data breaches, ransomware, and man-in-the-middle (MITM) attacks**.

### **Best Practices**

* Regularly update all software and operating systems.
* Use vulnerability scanners like Nessus for periodic assessments.
* Implement layered security measures, including firewalls and endpoint protection.

## **Recommendations**

* **Patch Management:** Apply updates and security patches for critical vulnerabilities.
* **Protocol Hardening:** Disable insecure protocols and enforce modern security standards (e.g., SMBv3, TLS 1.3).
* **Network Segmentation:** Isolate vulnerable systems to minimize exposure.
* **Access Control:** Follow a **least-privilege access model** to reduce exploitability.
* **Monitoring:** Use real-time monitoring tools to detect anomalies and potential threats.
* **Regular Scanning:** Schedule routine vulnerability assessments to ensure timely remediation.

1. **User Awareness Training:** Educate users on phishing and social engineering threats to reduce attack vectors.

## **Conclusion**

This project highlights the effectiveness of Nessus Essentials in **identifying and mitigating security risks** in a network environment. By following a structured approach—from setup to analysis and reporting—I was able to demonstrate the importance of **proactive vulnerability management**.

Organizations can significantly reduce their attack surface by leveraging tools like Nessus, implementing timely patches, and following best security practices.