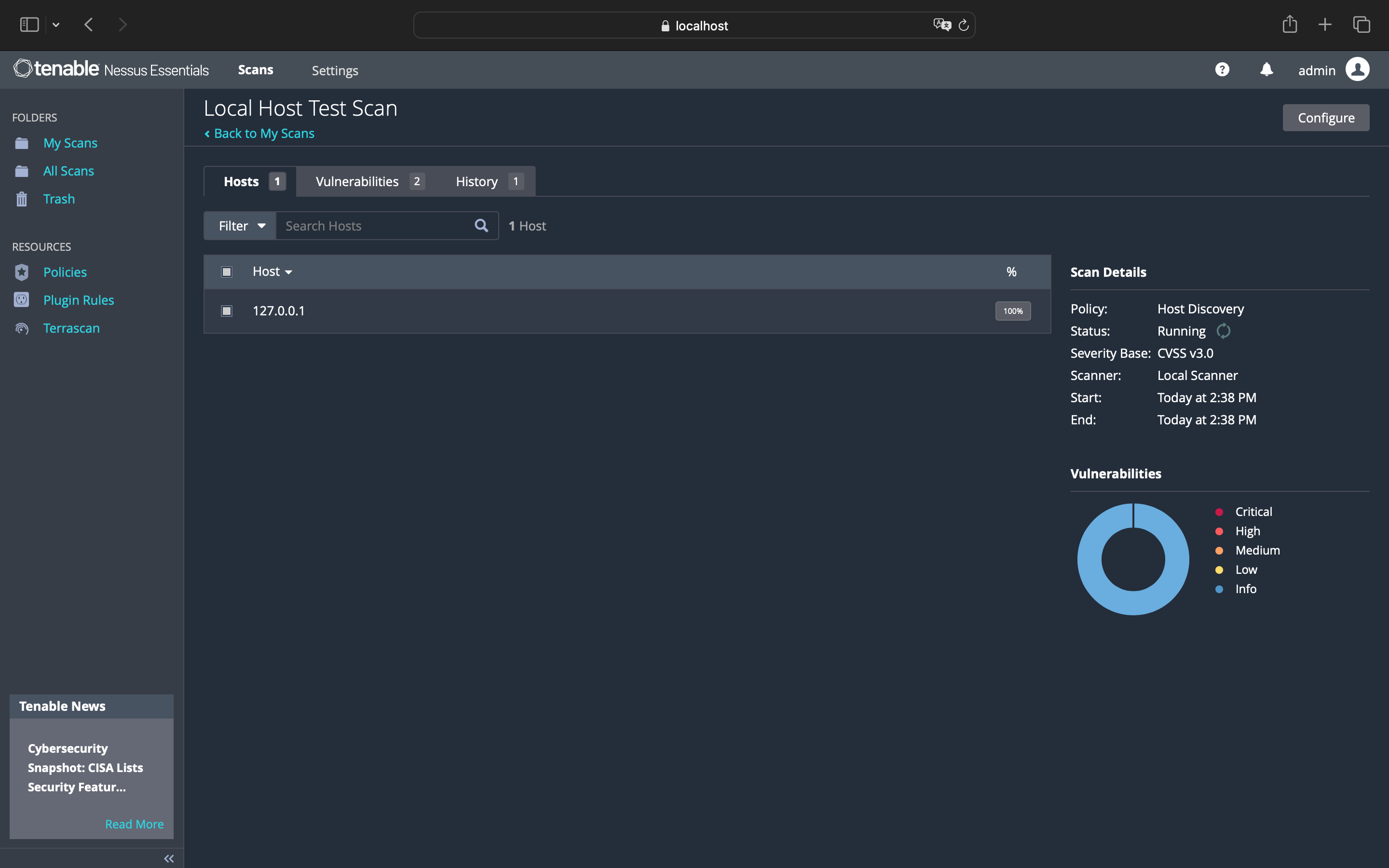
**Network Vulnerability Assessment Report**

**Introduction**

In this lab, I conducted a vulnerability assessment using Nessus to scan my local test network. The purpose of this scan was to identify security weaknesses, misconfigurations, and potential threats.

**Vulnerability Scan Setup**

To begin, I launched Nessus and configured a **Host Discovery** scan to analyze my local machine (127.0.0.1). The scan was executed using a local scanner, and I monitored its progress in the Nessus dashboard. The scan details, including policy, status, and timestamps, were displayed on the screen.



**Scan Results**

After completing the scan, Nessus presented a summary of vulnerabilities found on the system. Based on the results, no critical, high, medium, or low vulnerabilities were detected. The scan only identified **informational (INFO) findings**, which indicate general system details but do not pose an immediate security risk.

The two findings included:

1. **Nessus Scan Information** – This entry confirms that the scan was successfully conducted and recorded.
2. **Ping the Remote Host** – This indicates that the system responded to network requests, confirming that it is active.

**Credentialed vs. Non-Credentialed Scans**

* **Credentialed Scan**: This type of scan uses valid login credentials to access the system being tested. It provides deeper insights by checking system configurations, installed software versions, missing patches, and misconfigurations. Since it has insider access, it can detect vulnerabilities that an external attacker might not see.
* **Non-Credentialed Scan**: This scan does not use any login credentials and only assesses the system from an outsider’s perspective. It identifies vulnerabilities that could be exploited remotely, such as open ports, outdated services, and publicly accessible weaknesses. However, it lacks detailed visibility into system configurations and internal security risks.

A screenshot of a computer

Description automatically generated

**Risk Calculation**

Since no critical vulnerabilities were found, there was no need to calculate risk metrics such as Single Loss Expectancy (SLE), Annualized Rate of Occurrence (ARO), or Annualized Loss Expectancy (ALE). However, if vulnerabilities had been detected, I would have assessed their impact based on potential financial losses and likelihood of exploitation.

**Supply Chain Risk Assessment**

Although this scan focused on my local machine, it is important to evaluate third-party risks. Many organizations rely on external vendors for hardware and software, which introduces potential security risks. A proper **supply chain risk assessment** should be conducted to ensure that all third-party components are secure and do not introduce vulnerabilities into the network. Mitigation strategies may include:

* Conducting regular security audits on vendor products.
* Using only trusted suppliers with strong cybersecurity policies.
* Implementing strict access controls for third party integrations.

**Conclusion**

This vulnerability assessment confirmed that my local system did not have any critical security issues. However, continuous monitoring is necessary to ensure that new vulnerabilities do not emerge. Regular scans, combined with security best practices, will help maintain a strong security posture.