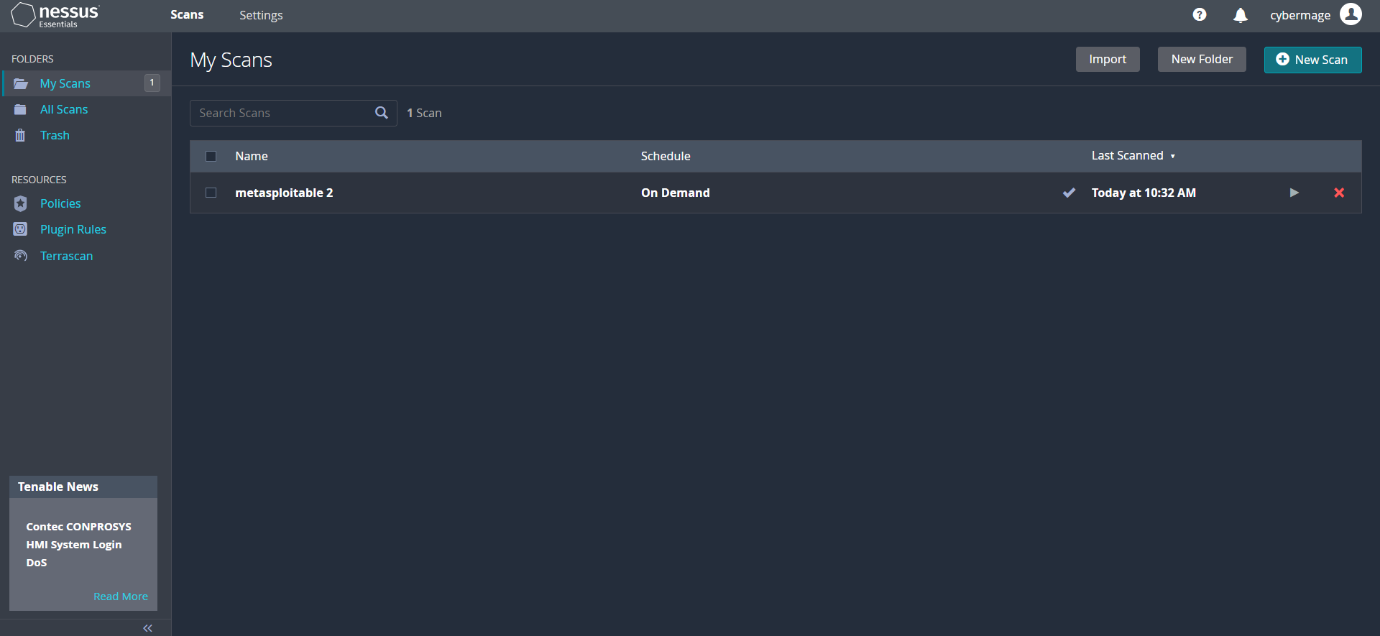
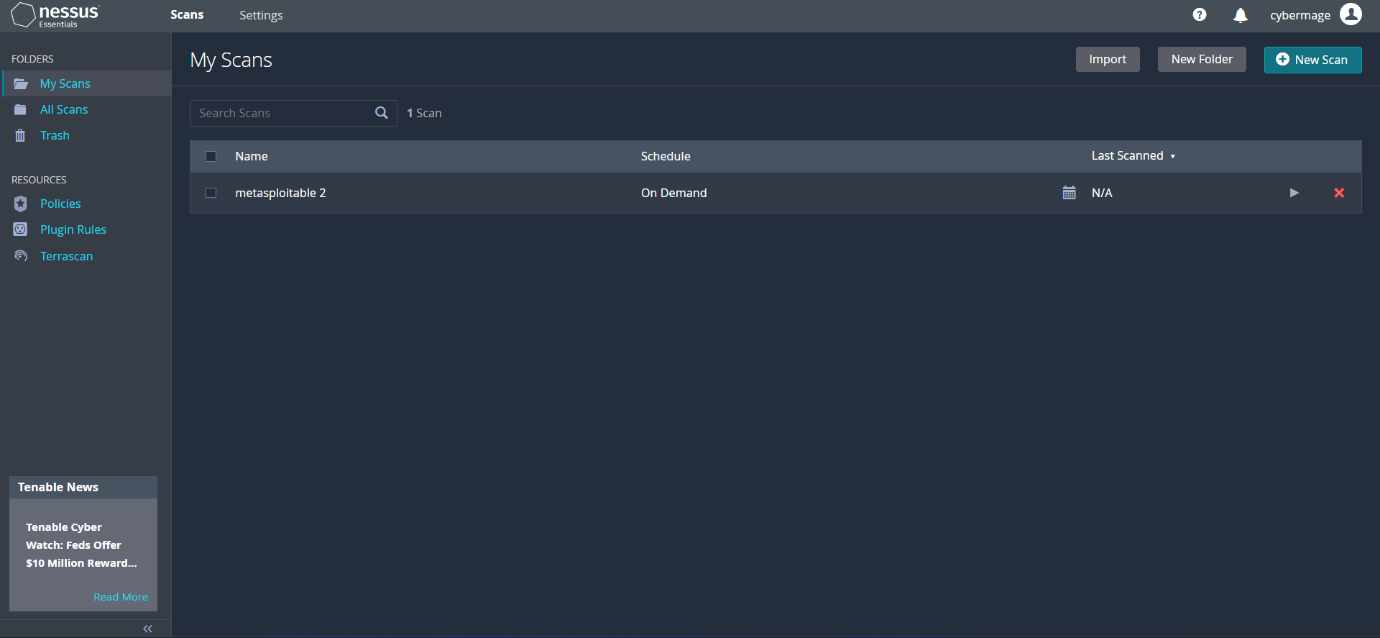
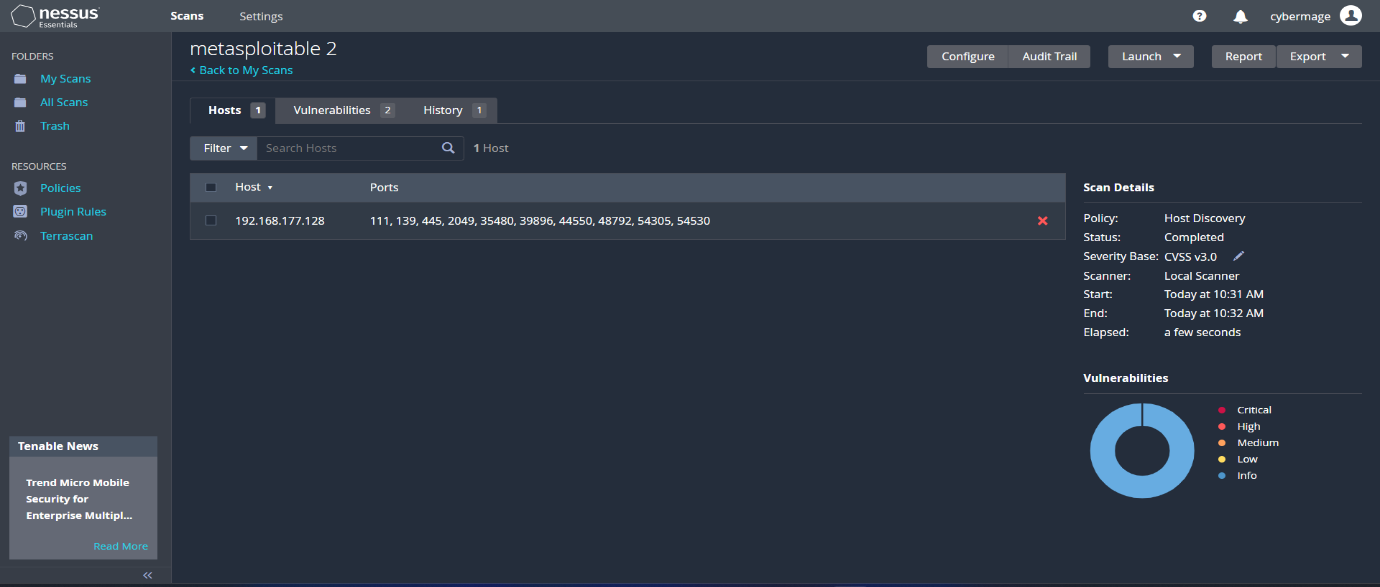
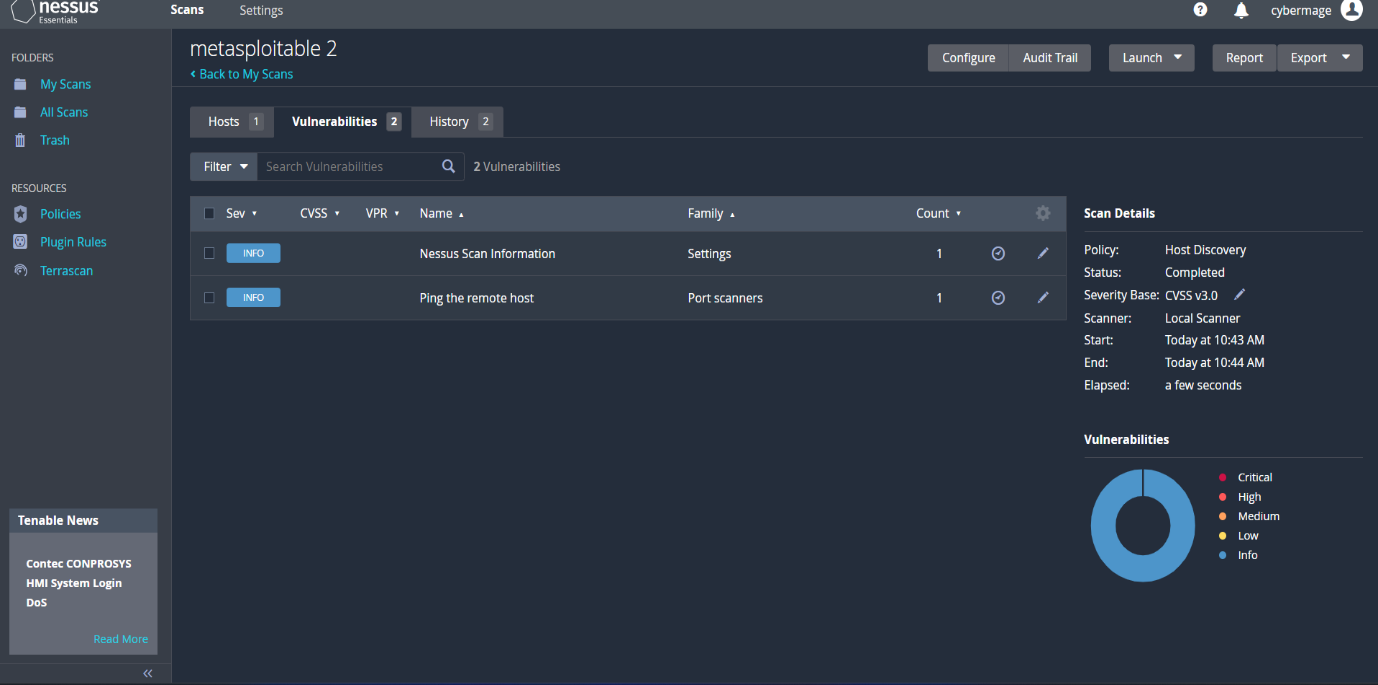
**Vulnerability Assessment Using Nessus (screenshots)**

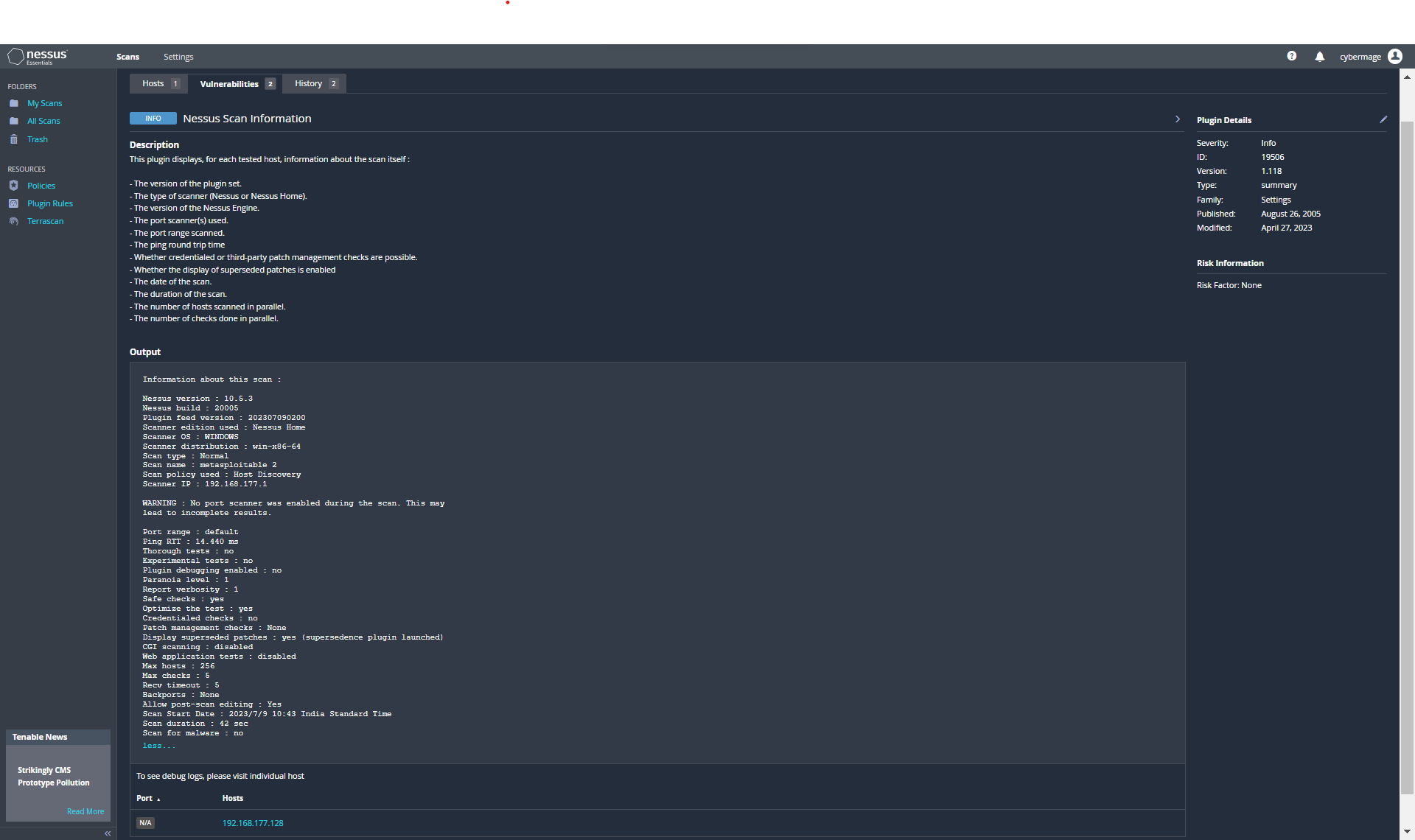
**Created a scan configuration in Nessus with Metasploitable 2 as the target.**

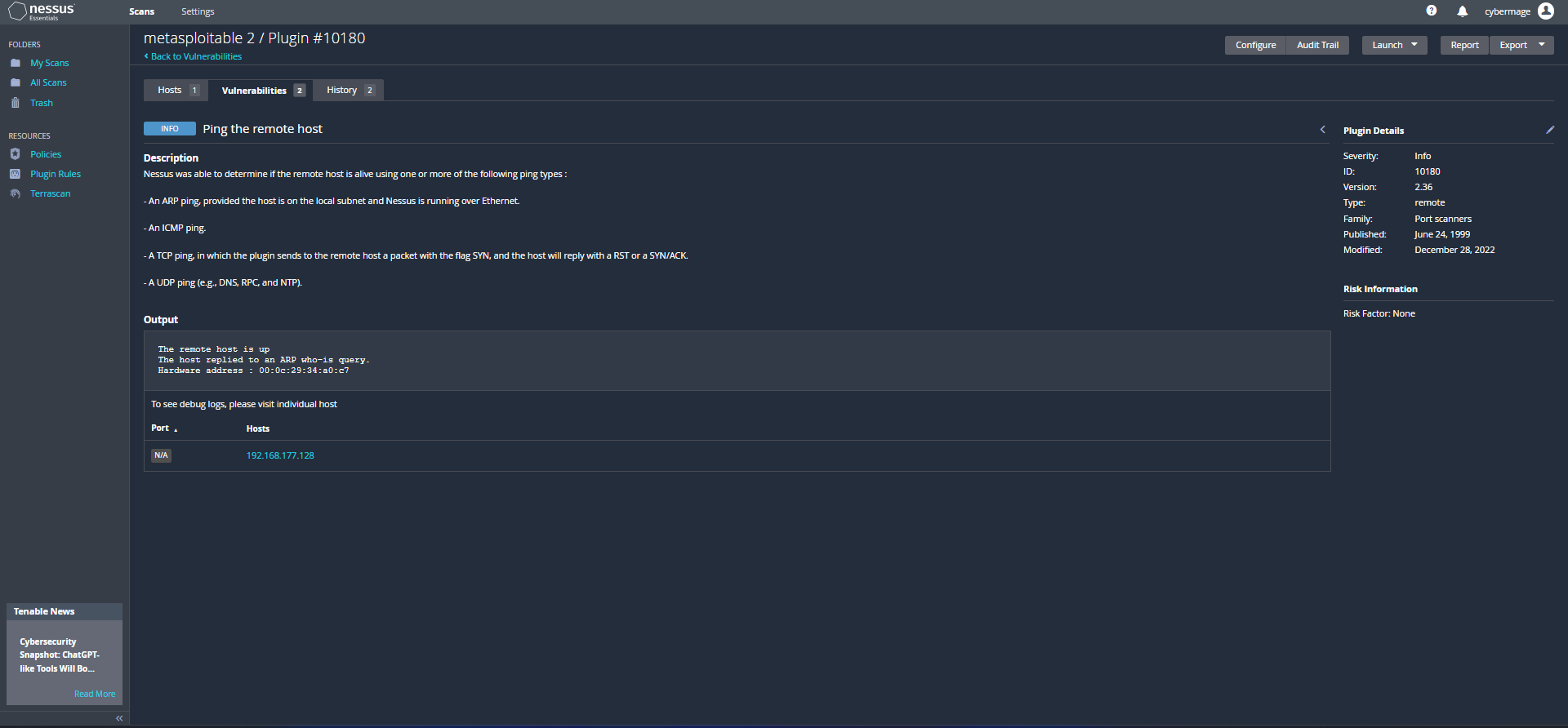


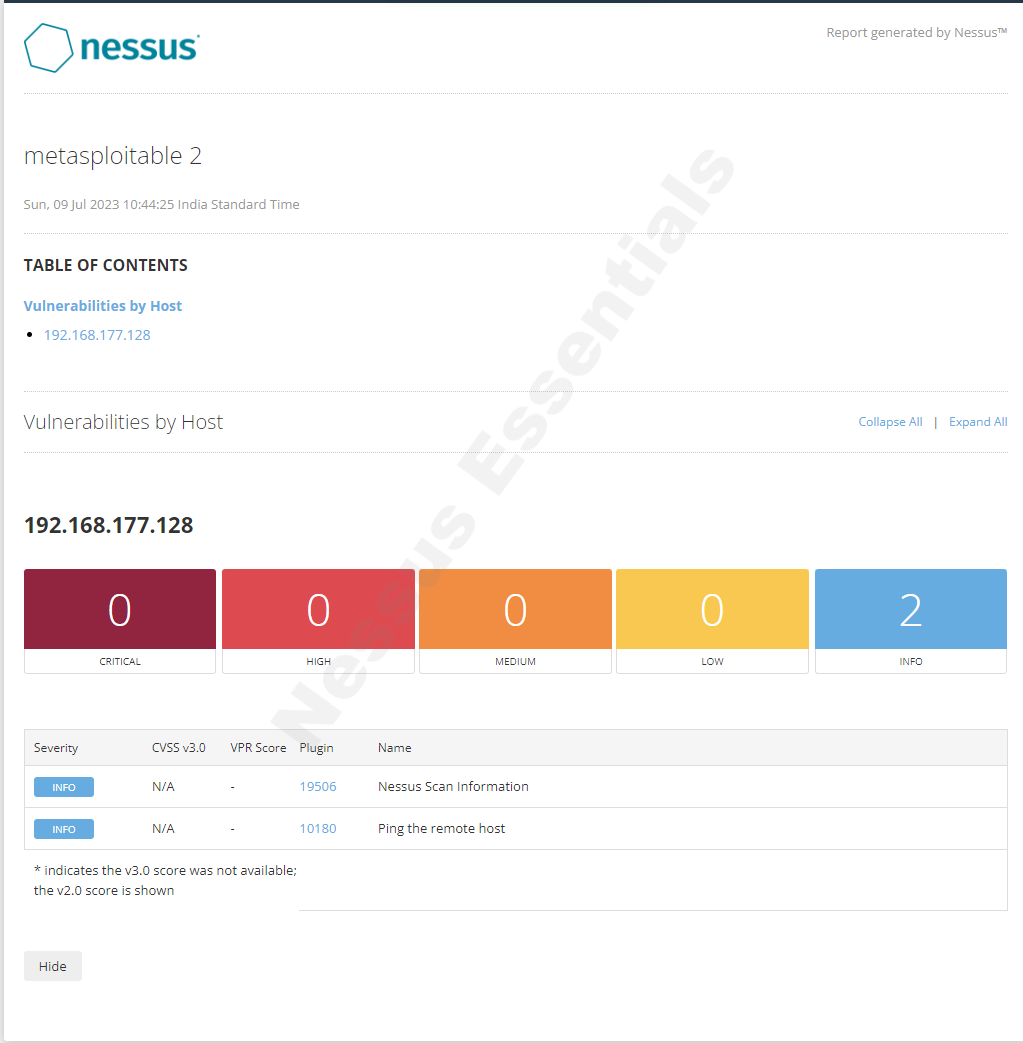
**Ran the Nessus scan on Metasploitable 2.**



**Analyze the scan results for identified vulnerabilities and their severity levels.**

****

****

**The Final Report Generated By Nessus**

**Nessus Vulnerability Assessment Findings Report**

The findings of the Nessus vulnerability assessment that was conducted on the Metasploitable 2 virtual machine. The assessment aimed to identify vulnerabilities, determine their severity levels, and provide recommended remediation actions for each vulnerability. The results of the assessment are summarized below.

1.Vulnerability Assessment Overview:

**Objective:** The objective of the vulnerability assessment was to evaluate the security posture of Metasploitable 2 and identify potential vulnerabilities.

**Methodology:** We used Nessus, a widely-used vulnerability scanner, to perform a comprehensive assessment of Metasploitable 2. The scan focused on identifying vulnerabilities across various services and applications running on the system.

2.Nessus Vulnerability Assessment Findings:

A total of **0** vulnerabilities were identified during the assessment.

Severity Levels: The vulnerabilities were classified into the following severity levels:

**Critical: [0]**

**High: [0]**

**Medium: [0]**

**Low: [0]**

3.Conclusion and Recommendations:

The Nessus vulnerability assessment did not reveal any vulnerabilities in the Metasploitable 2 virtual machine. This is an encouraging outcome, indicating that the system currently does not exhibit any security weaknesses based on the assessment performed. It is important to note that regular vulnerability assessments should still be conducted to proactively identify and address any potential vulnerabilities that may arise in the future. Although no vulnerabilities were identified, it is crucial to stay updated with security patches, follow vendor recommendations, and adhere to best practices for securing the Metasploitable 2 environment. This proactive approach helps maintain a robust security posture and safeguards against emerging threats.