TASK 3: - Basic Vulnerability Scan Report

This report documents the results of a basic vulnerability scan performed on my PC using Nessus Essentials.

SCAN SUMMARY:

Total vulnerability found	23
Critical	0
High	0
Medium	1
Low	0
Info	21
Mixed	1

Top identified vulnerabilities:

1. SMB signing not required

Vulnerability Name	SMB signing not required
Severity	Medium
Risk	May allow main-in-the-middle attacks by altering SMB traffic.
Fix	Enable SMB signing in Windows group policy.

2.SSL (Multiple issues)

Vulnerability Name	SSL (Multiple Issues)
Severity	Mixed
Risk	Outdated or Weak SSL/TLS configurations may expose encrypted data.
Fix	Disable weak ciphers and update TLS settings.

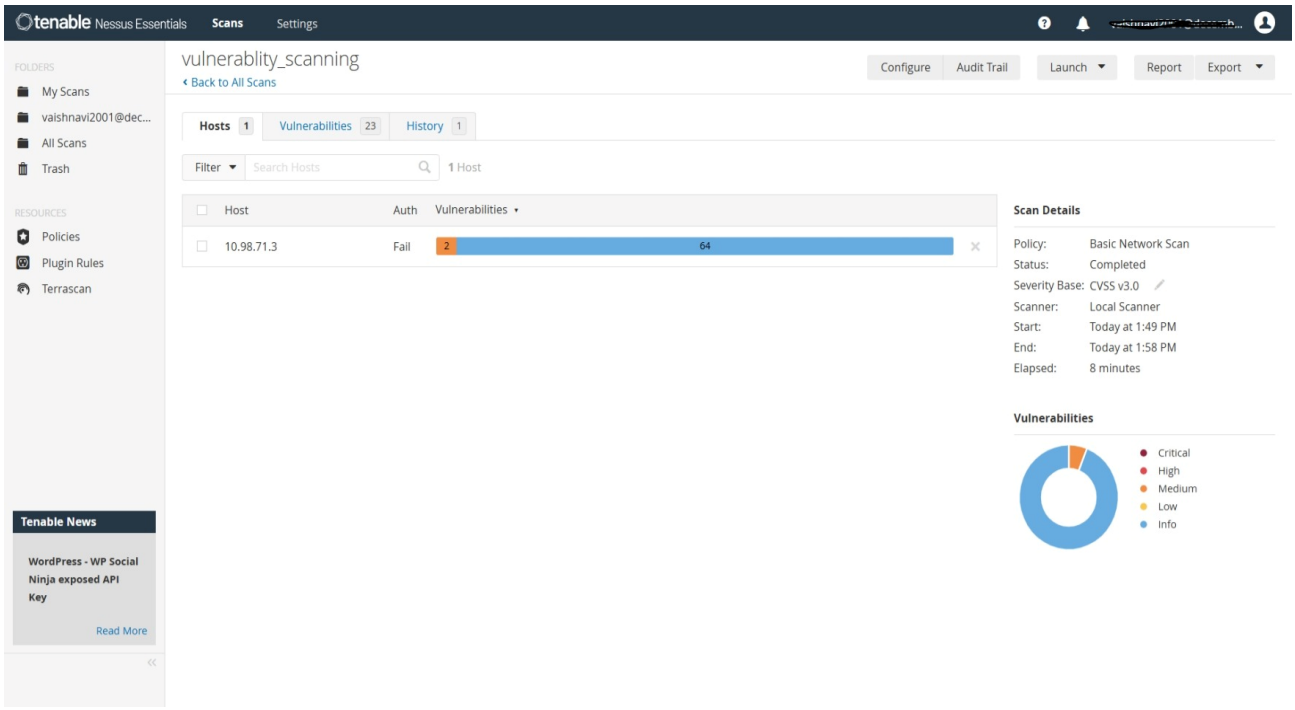
3.Service Detection /Enumeration Findings

Vulnerability Name	Service Detection/Enumeration Findings
Severity	Info
Risk	Information disclosure can aid attackers in mapping services.
Fix	Limit services exposure and disable unused services.

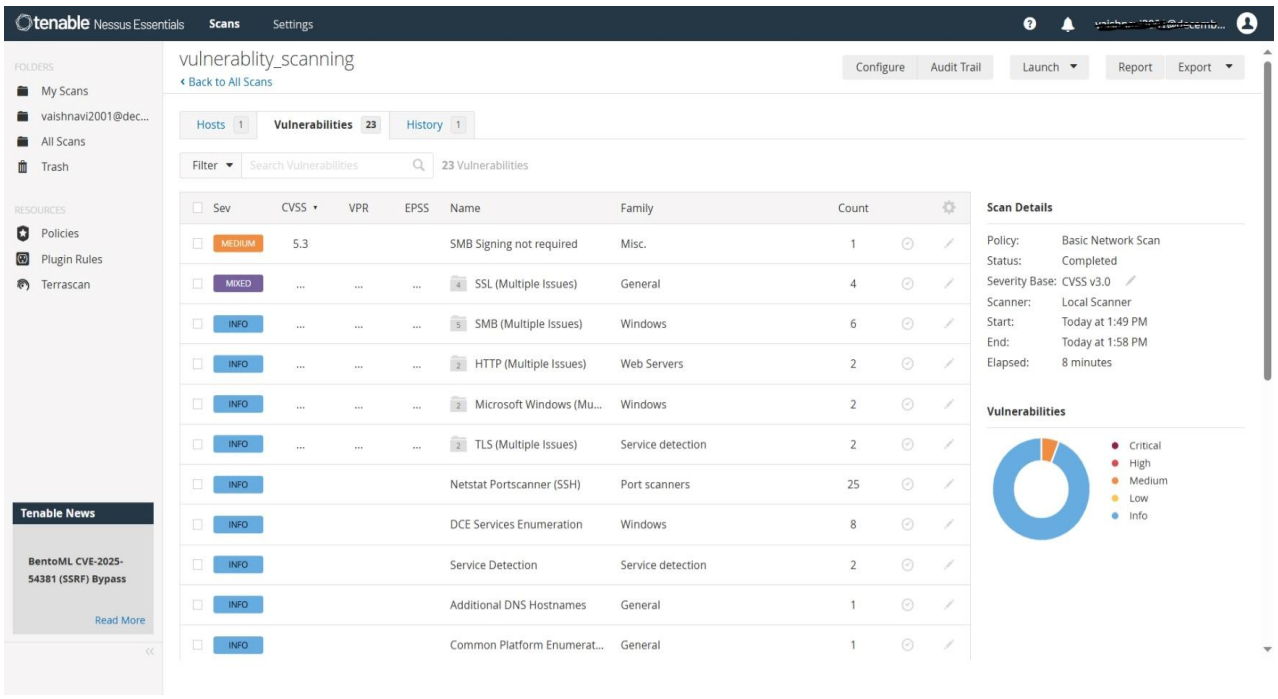
SCAN Evidence (Screenshots)

Below are screenshots from the Nessus Essentials vulnerability:

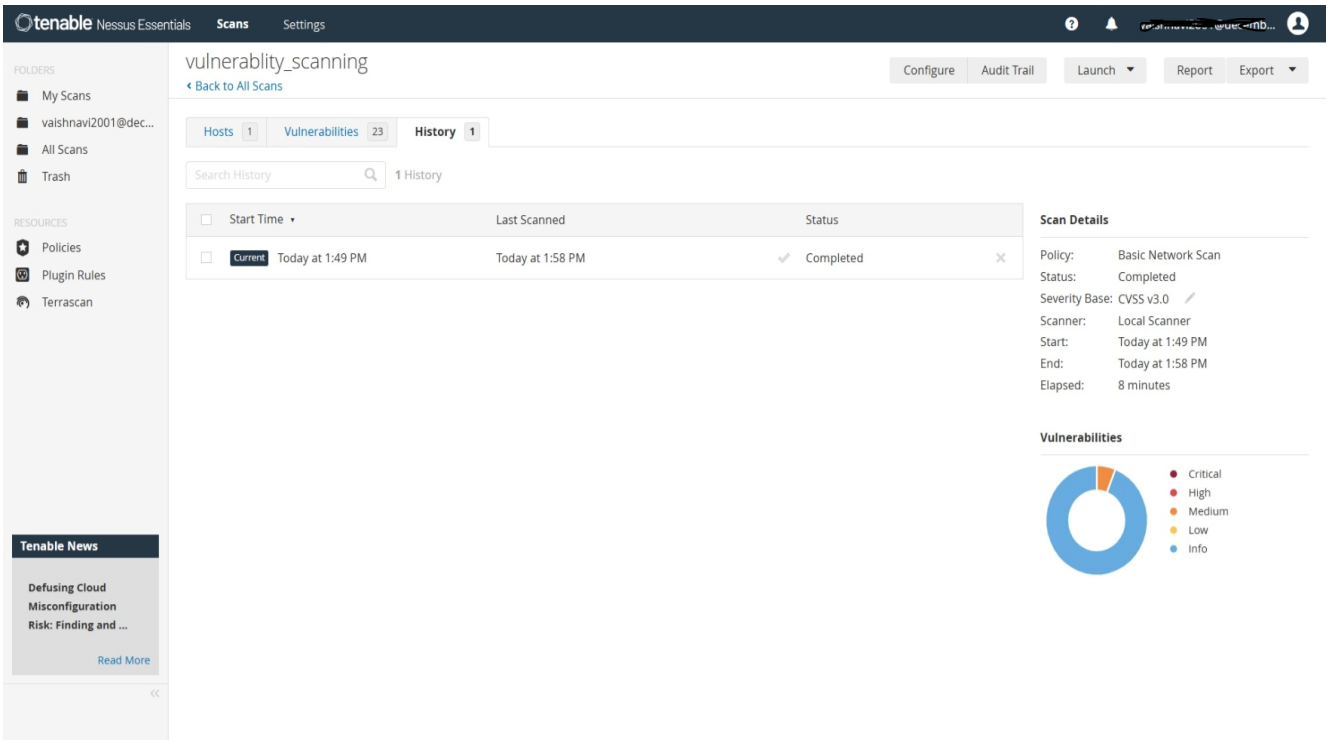
1: Host Scan Result



2.Vulnerability Summary page:



3.Scan History page



Outcome:

Through this task, I gained hands- on experience in running a vulnerability scan, analysing the results, and identifying potential risk on my PC. i also learned how to document findings and propose mitigation for issues like SMB signing misconfiguration, SSL weaknesses, and unnecessary service exposure.