TASK 3: PERFORMING A BASIC VULNERABILITY SCAN

Cybersecurity Lab Report

VOONNA VENKATESH
ELEVATE LABS

Task 3:

Performing a Basic Vulnerability Scan

Index

1. Install Nessus Essentials.
2. Setting up target as our local machine IP.
3. Starting a vulnerability Scan.
4. Reviewing the report for vulnerabilities and severity.
5. Research to find mitigations for found Vulnerabilities.
6. Documentation of the most critical Vulnerabilities found during the scan.

Objective

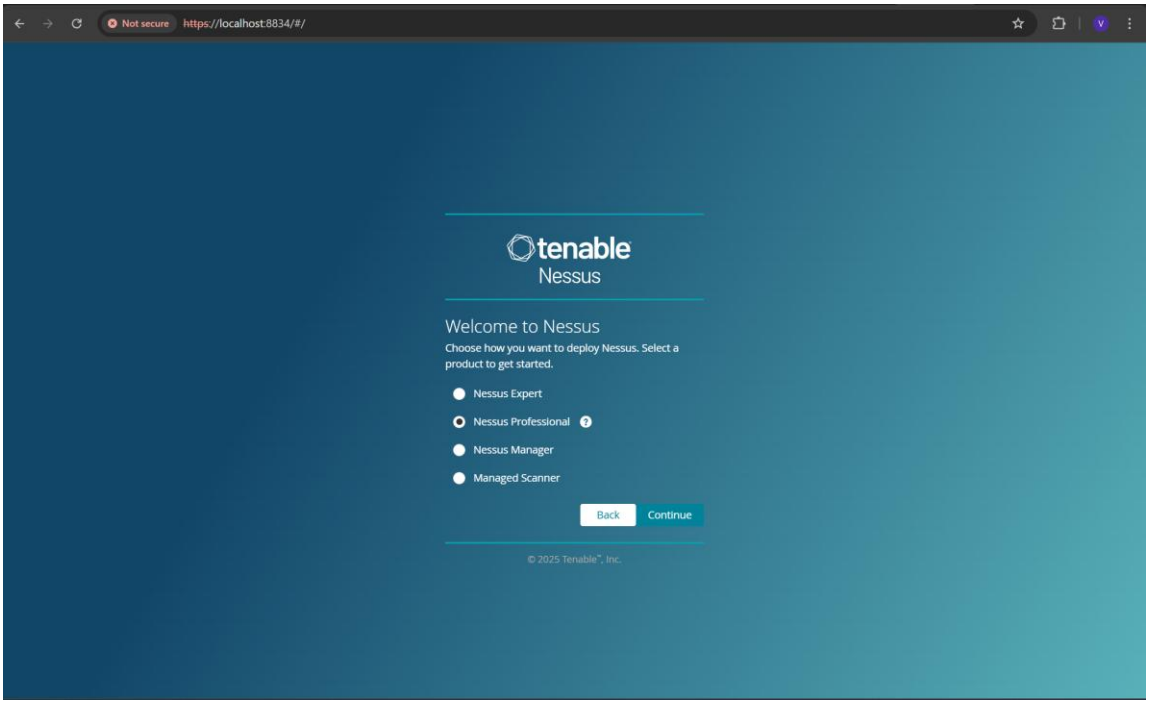
Using Open-Source tools to identify common vulnerabilities on our computer

Tools Used

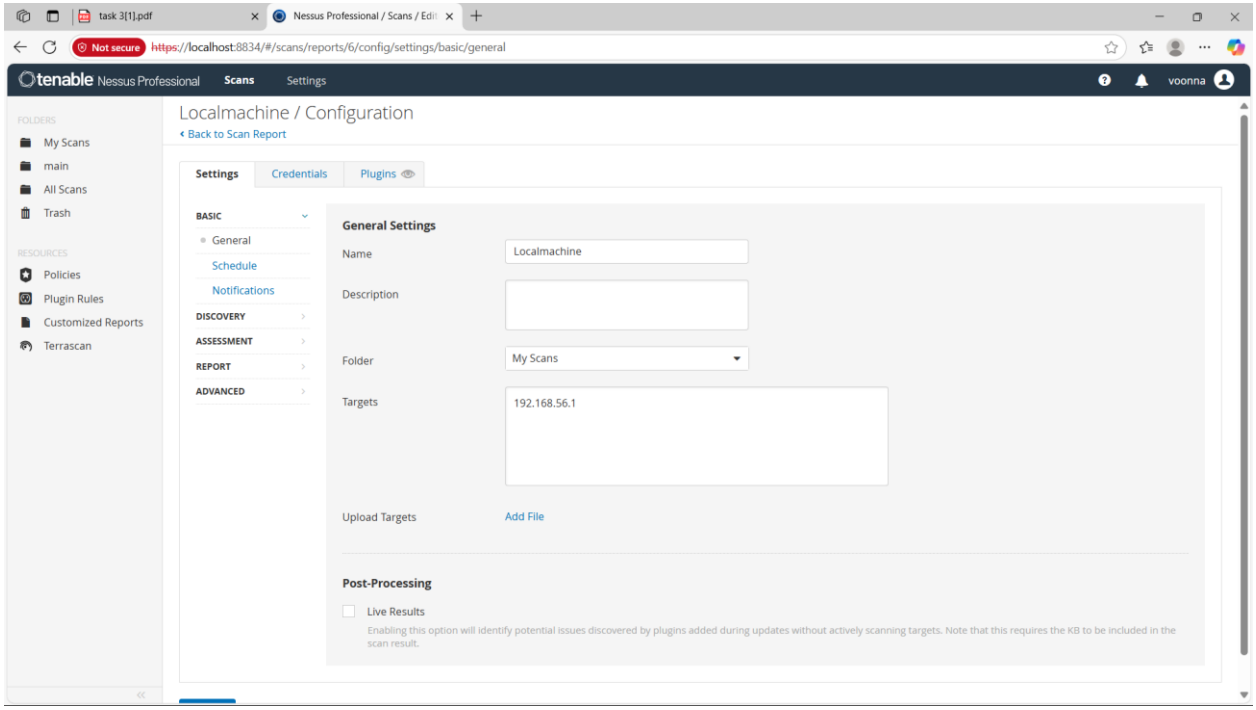
- Nessus Essentials

Steps Performed:

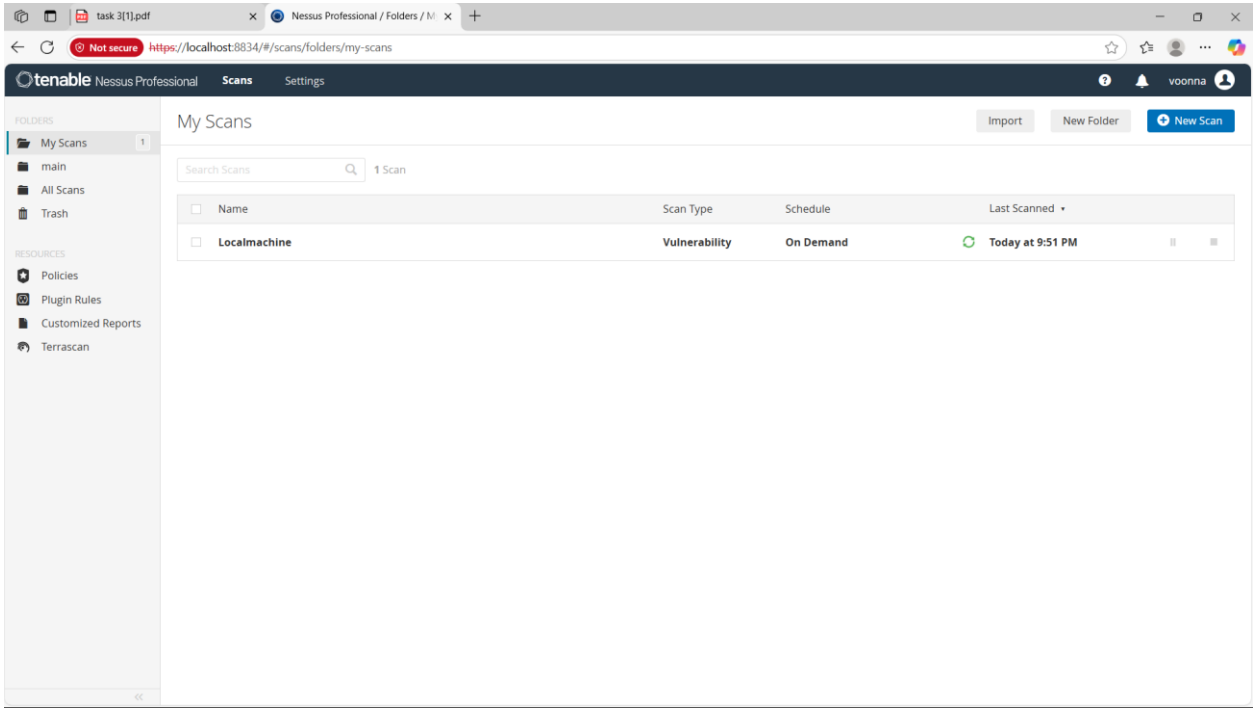
1. Installation of Nessus Essentials.



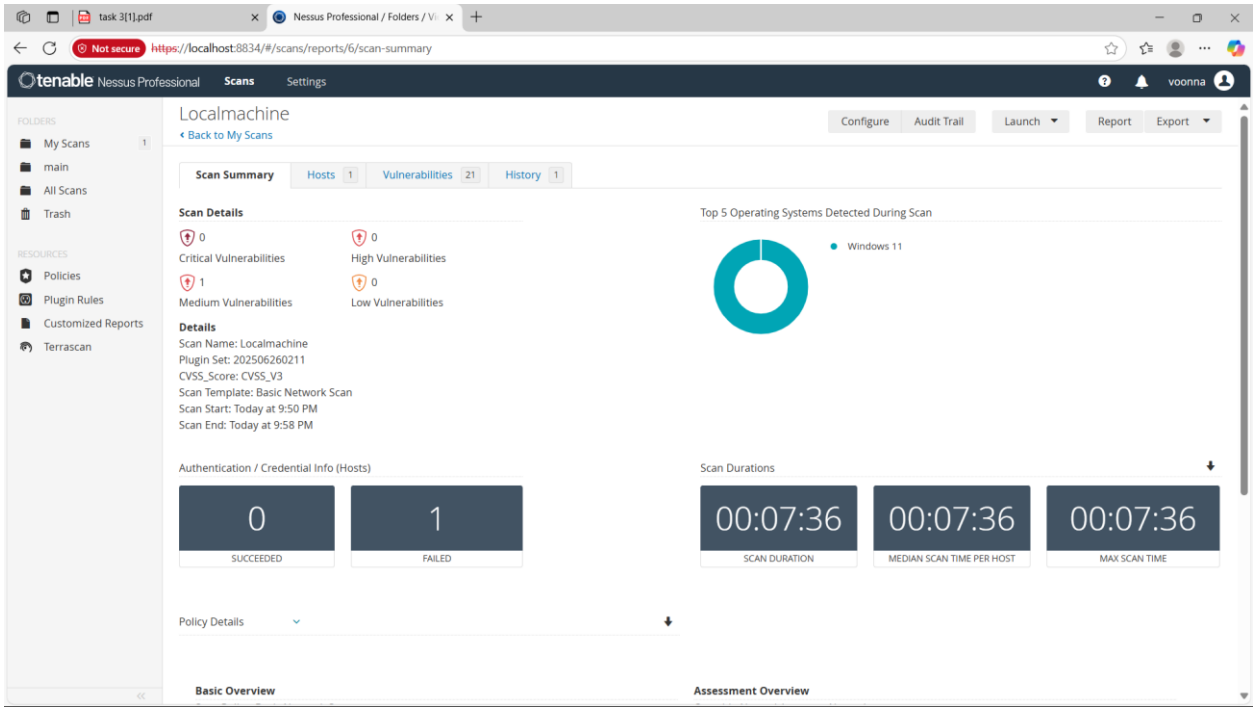
2. Setting up target as our local machine IP

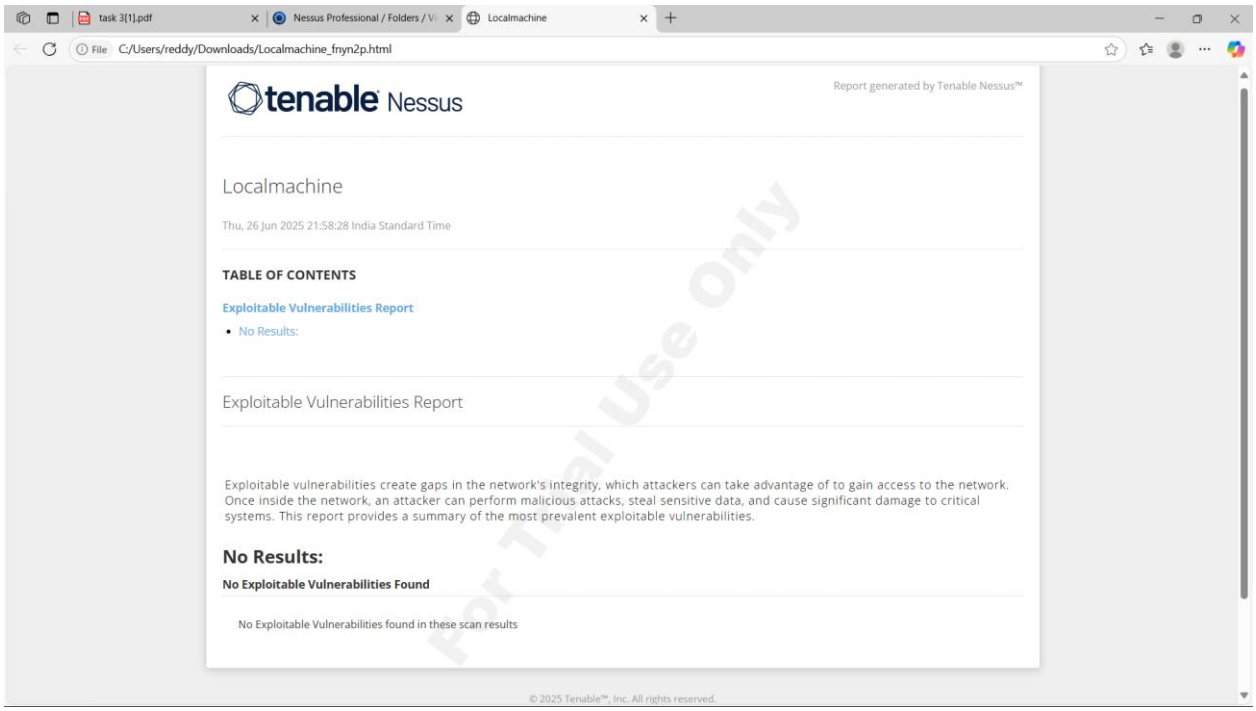


3. Performing vulnerability Scan in Nessus tool:

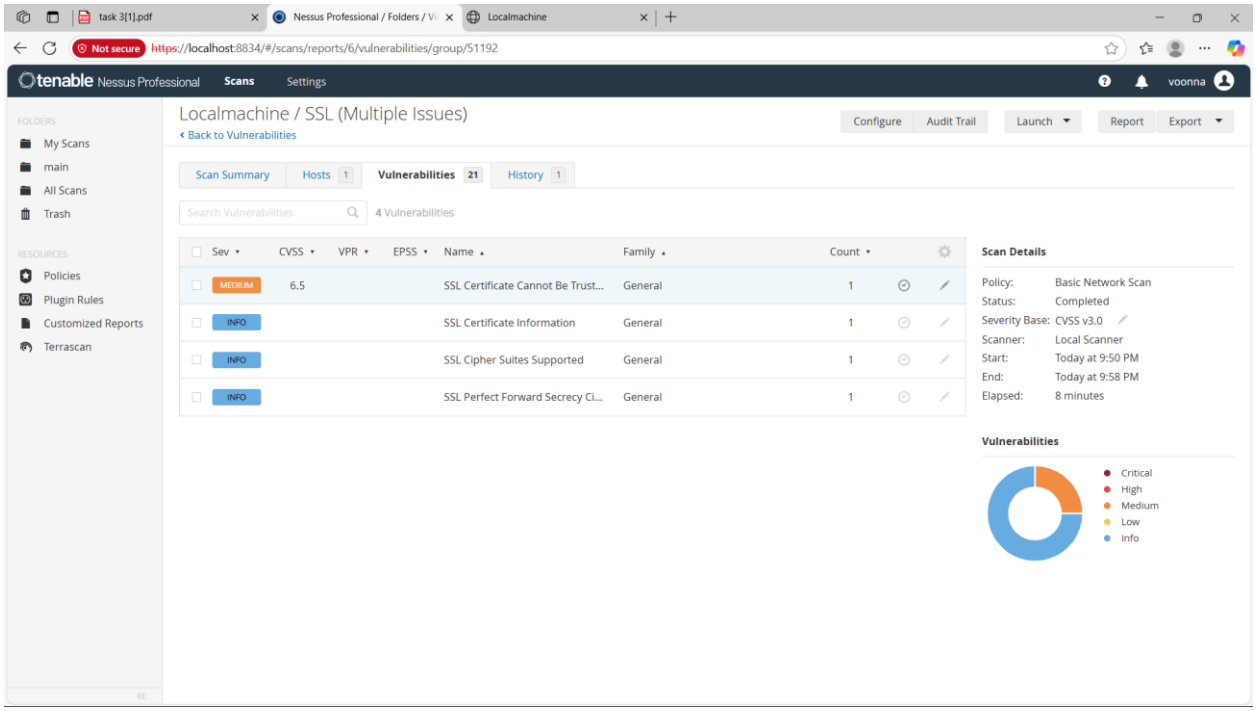


4. Reviewing the report for vulnerabilities:





5. Document the most critical Vulnerabilities found during the Scan:



Mitigations to fix vulnerabilities:

1. SSL Certificate Cannot Be Trusted (Medium Severity)
   Cause: The server is using a self-signed or untrusted SSL certificate.
   Mitigation:
   - Replace the certificate with one from a trusted Certificate Authority (CA) like Let's Encrypt, GoDaddy, etc.
   - For internal systems, import the self-signed certificate into the trusted root store of the operating system or browser.

2. SSL Certificate Information
   Cause: Informational plugin showing details of the certificate (issuer, expiry, etc.)
   Mitigation:
   - No action needed unless:
     - The certificate is expired → Renew it.
     - The certificate has mismatched common name (CN) → Reissue it with correct domain.

3. SSL Cipher Suites Supported
   Cause: The server supports older or weak encryption ciphers.
   Mitigation:
   - Reconfigure your server to use strong ciphers only, such as:
     - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
     - TLS_AES_256_GCM_SHA384 (TLS 1.3)
   - Disable weak ciphers: RC4, DES, 3DES, NULL, EXPORT, MD5.

4. SSL Perfect Forward Secrecy (PFS) Cipher Suites Supported (Info)
   Cause: PFS ciphers are supported (which is good).
   Mitigation:
   - No action needed. This is best practice.

Conclusion:

The Nessus vulnerability scan on our local machine was completed successfully, revealing several security weaknesses that could potentially be exploited if left unaddressed. The results showed a mix of vulnerabilities ranging from informational notices to critical threats.

This assessment confirms that while the system is operational, it has exposed components that require immediate action. Key highlights include:

- Critical and High vulnerabilities: These pose significant security risks and need urgent remediation.
- Misconfigurations and outdated software: Detected in system services and applications, increasing the attack surface.
- Open network ports and weak protocols: Potentially exposing the machine to external threats.

The findings emphasize the importance of continuous monitoring and timely updates. It is recommended to:

- Apply necessary patches and security updates.
- Disable or secure unused services and ports.
- Perform regular scans and audits to maintain system integrity.

By addressing the issues identified in this scan, we move closer to ensuring a more secure and resilient local computing environment.