Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

TASK – 3 BASIC VULNERABILITY SCANNING ON PC

Tools used: Nessus Essentials, Google, ChatGPT.

INTRODUCTION:

The purpose of this task was to perform a **basic vulnerability assessment** on my personal Windows 11 system using **Tenable Nessus Essentials**. Vulnerability assessment is the process of scanning a system to identify weaknesses, misconfigurations, or outdated software that attackers could exploit.

In this task, I installed Nessus Essentials, updated its plugin database, and configured a scan on my own machine (IP address 127.0.0.1 / 172.20.x.x). The scan was based on the **Basic Network Scan policy**, which checks for common security issues, including SSL/TLS configuration problems, outdated software, and insecure services.

The main objective of this assessment was to:

- Understand how vulnerability scanning tools work.
- Identify security issues on my system.
- Learn how to interpret severity scores (CVSS) and vulnerability details.
- Suggest basic remediation steps to improve security.

This report summarizes the scan results, highlights the most important vulnerabilities detected, and provides recommended fixes.

VULNERABILITY SCANNING:

Vulnerability scanning is the process of using automated tools to identify potential security weaknesses in computer systems, networks, or applications. The goal is to discover misconfigurations, outdated software, missing patches, and insecure settings before attackers can exploit them.

A vulnerability scanner, like **Nessus Essentials**, works by:

→ **Collecting system information** – it detects open ports, services, and software versions.

→ **Comparing against a database** – the tool checks this information against a known list of vulnerabilities (CVE database, plugin feeds).

→ **Generating a report** – the results are shown with severity ratings (Critical, High, Medium, Low, Info) based on the **CVSS scoring system**.

→ **Suggesting remediation** – most scanners also provide recommended fixes such as updating software, disabling weak protocols, or applying patches.

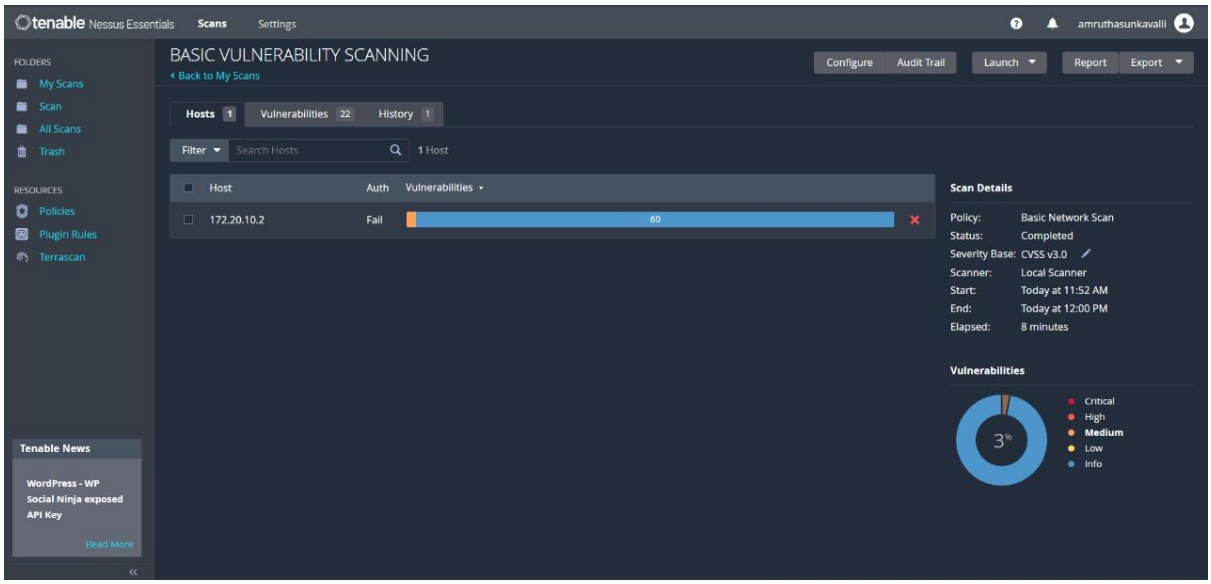
ADVANTAGES:

- Helps identify risks early.
- Saves time by automating security checks.
- Improves system hardening and compliance.
- Provides measurable data to track improvements over time.

DISADVANTAGES:

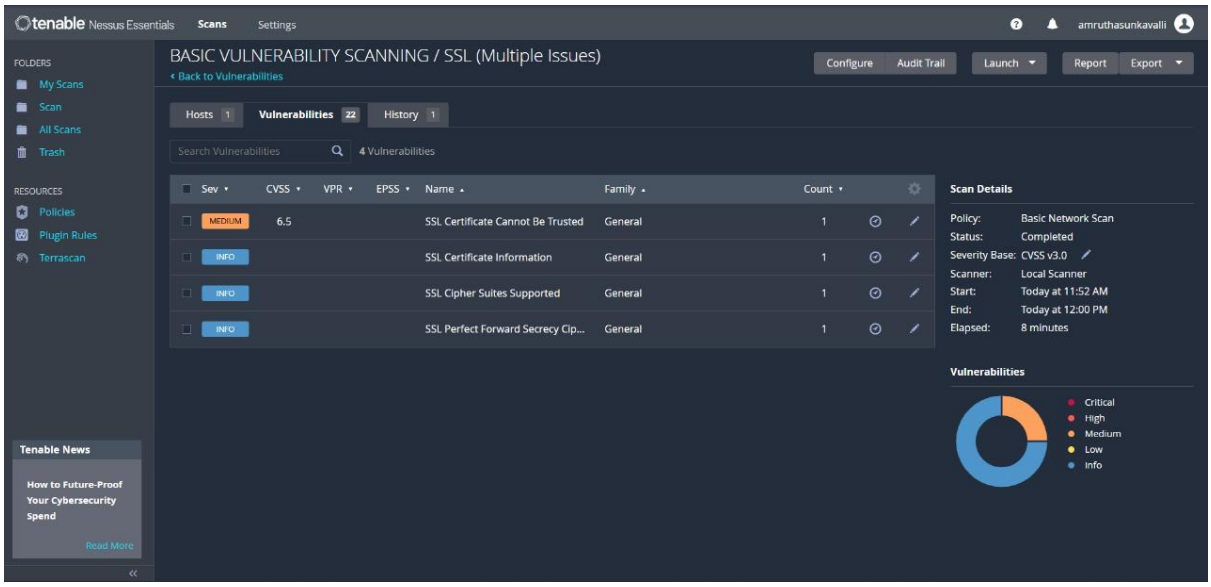
- It only finds vulnerabilities; it does not exploit them (that's penetration testing).
- Some results may be false positives.
- Effectiveness depends on keeping the vulnerability database up-to-date

BASIC VULNERABILITY SCANNING OVERVIEW (HOST FINDINGS AND VULNERABILITY SEVERITY:



Intern Name: S. Sai Amrutha
Mail: 240160226211.sunkavalli@gdgu.org

SSL/TLS VULNERABILITY IDENTIFIED (DETAILED ISSUES FROM TENABLE NESSUS ESSENTIALS SCAN):



VULNERABILITY 1: SSL CERTIFICATE CANNOT BE TRUSTED

- **Severity:** Medium (CVSS 6.5)
- **Description:** The SSL certificate presented cannot be fully trusted, which could allow attackers to intercept traffic or perform a “man-in-the-middle” attack.
- **Solution:** Replace the certificate with one signed by a trusted Certificate Authority (CA).

VULNERABILITY 2: SSL CERTIFICATE (INFORMATIONAL)

- **Severity:** Info
- **Description:** Nessus is reporting details of the SSL certificate, such as issuer, expiration, and algorithm. This is not a flaw but useful information.

VULNERABILITY 3: SSL CIPHER SUITES SUPPORTED (INFORMATIONAL)

- **Severity:** Info
- **Description:** Shows which SSL/TLS ciphers your system accepts. Weak ciphers should be disabled to prevent cryptographic attacks.

VULNERABILITY 4: SSL PERFECT FORWARD SECRECY (INFORMATIONAL)

- **Severity:** Info
- **Description:** Lists ciphers that support Perfect Forward Secrecy. This is generally good, but Nessus flags it for review.

COMMON VULNERABILITY SCORING SYSTEM (CVSS):

CVSS stands for **Common Vulnerability Scoring System**.
It is an open standard used to measure the severity of computer system vulnerabilities. CVSS assigns each vulnerability a numerical score ranging from 0 to 10, which security teams use to prioritize which issues should be addressed first.

CVSS SCORE RANGE:

Score Range	Severity Level	Meaning
9.0 – 10.0	Critical 🔴	Easily exploitable, severe impact, needs urgent fix.
7.0 – 8.9	High 🟠	Dangerous, may allow compromise with some conditions.
4.0 – 6.9	Medium 🟡	Moderate risk, could be exploited but is less critical.
0.1 – 3.9	Low 🔵	Minor issue, unlikely to be exploited.
0.0	Informational ⚪	No direct risk, just system information.

The vulnerability in my scan with a score of **6.5** is considered **Medium severity**, meaning it could pose a real risk but is not immediately catastrophic.

RISK ASSESSMENT:

Risk assessment in cybersecurity is the process of identifying, analysing, and evaluating potential threats and vulnerabilities that could affect the confidentiality, integrity, and availability of information systems. Its purpose is to understand the likelihood of a cyber threat occurring and the potential damage that would result if it were to happen.

STEPS IN CYBER RISK ASSESSMENT:

1. **Identify Assets:**
   Determine which systems, data, applications, and networks need protection—for example, personal data, financial information, or critical system files.
2. **Identify Threats and Vulnerabilities:**
   - Threats may include malware, phishing attacks, insider threats, or data breaches.
   - Vulnerabilities are weaknesses such as outdated software, weak passwords, or unpatched operating systems.

3. **Analyse Risks:**
   Assess the **likelihood** of each threat exploiting a vulnerability and the **impact** it would have on the organization or individual.
4. **Evaluate and Prioritize Risks:**
   Classify risks as **High, Medium, or Low** based on their severity. High-priority risks require immediate action, while low-priority risks can be monitored.

5. **Mitigation and Control:**
   Apply security measures to reduce risks, such as:
   - Installing updates and patches
   - Using firewalls and antivirus software
   - Enforcing strong password policies
   - Educating users about phishing attacks
6. **Monitoring and Review:**
   Risk assessment is not a one-time activity. Continuous monitoring and regular reassessments are essential because new threats constantly emerge.

IMPORTANCE OF RISK ASSESSMENT IN CYBERSECURITY:

- Protects sensitive information from unauthorized access.
- Reduces chances of financial loss, legal penalties, and reputational damage.
- Ensures compliance with security standards and regulations.
- Builds a stronger security posture against evolving cyber threats.

CONCLUSION:

The vulnerability assessment performed with **Nessus Essentials** successfully demonstrated how automated tools can identify weaknesses in a system. By scanning my Windows 11 machine, I was able to detect one **medium severity issue** (SSL Certificate Cannot Be Trusted, CVSS 6.5) along with several **Informational findings** related to SSL configuration.

This task helped me understand the importance of **vulnerability scanning** in cybersecurity. I learned how to:

- Install and configure a vulnerability scanner.
- Run a scan on my own system.

- Interpret results using severity levels and CVSS scores.
- Research remediation steps to address detected issues.

Even though my system did not have any **Critical or High-risk vulnerabilities**, the findings highlight that even small configuration issues can create opportunities for attackers. Regular scanning, timely patching, and applying recommended fixes are essential steps in maintaining system security.

Overall, this task gave me practical hands-on experience in vulnerability assessment and strengthened my understanding of how security tools are applied in real-world scenarios.

****