**1. Student Information**

* **Course Code**: CSCS3553
* **Instructor's Name**: Prof.Hassan Rauf
* **Group Members with their Registration Number (If applicable)**:
  + **Name 1**: Asad Mushtaq(G1F22UBSCS075)
  + **Name 2**: Hunain Farooq(G1F22UBSCS244)

**2. Project Details**

* **Project Title**: Security Vulnerability Scanner\_: Develop a program to scan for security vulnerabilities in an operating system.
* **Project Type** (Choose one):
  + **Other (Security System/Network Security Tool)"** it is a good way to describe it. The primary goal of my project is to scan and assess the security of an operating system, making it more of a **security tool** rather than a system modification or simulation. You could specify it as: System Security Project.
* **Technologies Used**:

**Python**

* **Primary Language**: Python is a great choice for this project due to its readability, ease of use, and powerful libraries. You can use Python to interact with the operating system, execute system commands, parse system information, and interact with external services.
* **Why Python?**
  + **Cross-Platform**: Python works seamlessly across both Windows and Linux systems.
  + **Libraries**: Python has extensive libraries to make this process simpler (e.g., psutil, subprocess, requests, nmap, etc.).
  + **Quick Development**: It allows for faster prototyping and testing.

**3. Project Overview**

**Project Objective/Goal:**

This project aims to develop a **Security Vulnerability Scanner** that detects open ports, outdated software, system misconfigurations, and potential malware threats. The scanner will help users identify and mitigate security risks in their system.

**Key Features/Functionalities:**

* Open port scanning
* Outdated software detection
* Misconfiguration analysis
* Basic malware signature scanning
* Graphical User Interface (GUI) for ease of use
* Report generation for security audit
* Stop scan functionality for user control

**Operating System Concepts Demonstrated:**

☑ Process Management  
☑ Memory Management  
☑ File System Implementation  
☐ Synchronization  
☑ Deadlock Handling  
☑ Virtualization  
☑ Multithreading  
☑ Security  
☐ Other: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**4. Project File Submission**

**Source Code Link:**  
[Insert link to repository if using GitHub, GitLab, etc. (e.g., <https://github.com/username/project>)]

**Executable File/Program (If applicable):**  
☑ Attached executable file (Upload link or attachment for submission)

**5. Additional Information (Optional)**

**Challenges Faced During the Project:**

* Handling large-scale system scans without freezing the GUI.
* Implementing efficient malware scanning to reduce execution time.
* Ensuring accuracy in detecting system vulnerabilities.

**Future Improvements/Extensions:**

* Integration with VirusTotal API for real-time malware detection.
* Adding advanced threat analysis for network traffic monitoring.
* Scheduling automatic periodic security scans.
* Implementing AI-based security vulnerability prediction.

**6. Acknowledgments**

**Any Help/Resources Used:**

* Online cybersecurity tutorials and documentation.
* Python libraries such as socket, subprocess, and tkinter.
* GitHub repositories for reference on security tools.

**7. Declaration**

I hereby declare that the project submitted is my own work and has not been plagiarized. I also acknowledge the help from any resources mentioned above.

**Student Signatures:**

* **Name:** Asad Mushtaq **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
* **Name:** Hunain Farooq **Signature:** \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**8. Submission Date**

**Date of Submission:** 28-0-25

**9. Instructor Comments (For Instructor Use)**

**Feedback/Comments:**