Group 22 CAPSTONE project

I.Project Name:

Agentic AI Penetration Testing Framework

II.Project Objectives:

The objective of this project is to design and implement an Agentic AI–driven Penetration Testing Framework that extends and improve the current proof-of-concept. The student team will develop a multi-agent architecture covering reconnaissance, enumeration, exploitation, and post-exploitation, while improving reliability by reducing hallucinations and redundant scans. The system will provide continuity across sessions, generate context-aware exploit strategies, and deliver automated postexploitation analysis with structured reporting. The working prototype should demonstrate greater automation, accuracy, and usability for AI-assisted penetration testing.

III.Project Overview:

This is a challenging project that will require students to apply cybersecurity knowledge, penetration testing methodologies, and AI/agent-based system design principles. The project scope includes extending a proof-of-concept Agentic AI penetration testing pipeline into a more complete and reliable framework. Students will begin by reviewing existing penetration testing standards and methodologies (e.g., PTES, OWASP) and analyzing the current proof-of-concept system to identify its limitations. Based on this review, the team will design a multi-agent workflow that integrates reconnaissance, enumeration, exploitation, and post-exploitation. Major requirements include implementing command validation to reduce hallucinations, developing memory and context management for continuity, integrating vulnerability knowledge through Retrieval-Augmented Generation (RAG), and adding a post-exploitation and reporting agent. The envisioned execution process involves building and iteratively testing the system within a controlled lab environment, gathering feedback from penetration testers, and refining the workflow to improve automation, accuracy, and usability. The final deliverable will be a working prototype with structured documentation and a comprehensive report of findings and recommendations.