SYSC 4907 – Fall 2026/Winter 2027

Supervisor	Nafiseh Kahani
Co-supervisor	
Course section	SYSC 4907 Y
Project ID	
Project title	Agentic AI Penetration Testing Assistant
Project description	Build an AI agent that helps to perform a penetration-testing workflow inside a closed lab environment. The agent(s) can plan the test, choose from approved tools, run scans against intentionally vulnerable machines, summarize findings, map vulnerabilities to risk levels, and generate a professional security report. The agent should also introduce new ways of testing rather than only relying on existing vulnerability-scanning tools. For example, it can help to design custom test cases, suggest manual verification steps, compare results from multiple tools, identify gaps in automated scans, and explain how a vulnerability could be confirmed safely inside the lab. The project should not target real systems, public IPs, university networks, or third-party websites. It should only work against pre-approved lab targets such as OWASP Juice Shop, DVWA, or Metasploitable 2. OWASP Juice Shop is designed for security training and includes OWASP Top 10 vulnerabilities, DVWA is intended for legal classroom security practice, and Metasploitable 2 is an intentionally vulnerable VM for testing common vulnerabilities.
Program(s)	Computer Systems Software
Maximum number of students	3
Meeting time with supervisor (optional)	
Do you want the student to contact you before the office assign this project to them ? (Yes/No)	