Sponsor Project Nomination Form

Sponsor Organization Name: George Mason University

Sponsor POC:

Name & Title	Zhengdao Wang
Location	Fairfax, VA
Phone	703-993-1578
Email	zwang52@gmu.edu

Sponsor Technical SME:

Name & Title	Md Faisal Ahmed
Location	Fairfax, VA
Phone	571-663-7772
Email	mahmed75@gmu.edu

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 post-exploitation 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.

IV. Major Deliverables

a. Required Deliverables (must haves)

Deliverable	Due Date
Draft Agentic AI for Recon & Enumeration Modules	Mid Fall
Extended Framework with Exploitation & Post-Exploitation Agents	Late-Fall
Draft Evaluation Report	Early Spring
Final Prototype and Report and AI Software Package	Late Spring

b. Desired Deliverables (nice to haves)

Deliverable	Due Date
Agentic AI Pentest Framework User Guide	Late Spring
Research Paper for Conference Submission	Late Spring

V. Hours / Week

2 hours/week. Note: we will make the Sponsor available for review and approval of project deliverables, we will have the SME available for weekly student meetings and reviews.

VI. Project Resources

Resource Type	Description	Provided By (GMU or Sponsor)
Compute	Virtualized penetration testing environment (attacker and victim VMs running on cloud infrastructure)	GMU
Software	Open-source penetration testing tools (Kali Linux, Nmap, Metasploit, Burp Suite Community) and LangGraph framework, LLM API access (Azure OpenAI, Anthropic, etc.)	Freely available
Data / Information	Vulnerability databases (ExploitDB, NVD, CWE), redacted vendor documentation for RAG integration	Freely available
Other	Documentation, research articles, and technical guidance from security experts	Freely available, or GMU library

VII. Student Team: Skills and Size

a. Required Skills

Students should be familiar with the principles of penetration testing, common cybersecurity concepts, working knowledge of Python programming and basic understanding of Linux environments.

b. Desired Skills

Experience with penetration testing tools (e.g., Nmap, Metasploit, Burp Suite, Wireshark), familiarity with AI/LLM frameworks (e.g., LangChain, LangGraph, Hugging Face), and exposure to Retrieval-Augmented Generation (RAG) concepts and knowledge of cloud platforms (Azure/AWS/GCP) and prior experience with multi-agent systems or security research will be a plus. Students should have a strong desire to learn how to integrate AI with cybersecurity tasks and to safely and effectively conduct penetration testing in controlled environments.

c. Team Size

Ideally, a student team of 4-6 students will support the project.

VIII. Citizenship

No.