

I. IDENTIFICATION DATA

Thesis name:	Click here to enter text.
Author's name:	Muris Sladic
Type of thesis :	master
Faculty/Institute:	Faculty of Electrical Engineering (FEE)
Department:	Computer Science
Thesis supervisor:	Carlos Catania
Supervisor's department:	Computer Science, Faculty of Engineering, UNCuyo. Mendoza, Argentina

II. EVALUATION OF INDIVIDUAL CRITERIA

Assignment	challenging
<i>Evaluation of thesis difficulty of assignment.</i>	
<p>The assigned project was notably demanding, primarily due to the incorporation of cutting-edge Language Model (LLM) technology. Utilizing such a new and complex technology presented significant challenges. Despite these difficulties, the candidate successfully developed multiple innovative tools that enhanced the engagement and effectiveness of honeypots. This achievement not only demonstrates the candidate's technical prowess but also their ability to navigate and apply emerging technologies in practical, impactful ways.</p>	

Satisfaction of assignment	fulfilled
<i>Assess that handed thesis meets assignment. Present points of assignment that fell short or were extended. Try to assess importance, impact or cause of each shortcoming.</i>	
<p>The thesis admirably fulfills the assigned task, meeting all primary goals with exceptional quality. The development of tools utilizing LLM technology to emulate the behavior of various systems—Linux shell, MySQL, POP3, and HTTP—demonstrates a comprehensive approach to enhancing honeypot engagement and realism. Furthermore, the creation of the LLM attacker, a tool designed to simulate human attackers, indicates a robust testing and evaluation framework that complements the development of the emulators.</p>	

Activity and independence when creating final thesis	A - excellent.
<i>Assess that student had positive approach, time limits were met, conception was regularly consulted and was well prepared for consultations. Assess student's ability to work independently.</i>	
<p>The student consistently exhibited a proactive attitude throughout the duration of the thesis project. This proactive approach was evident in all phases of the project, including coding, writing, and experimental design, indicating a strong, positive work ethic. Regarding time management, the student met all designated deadlines effectively. Their ability to act independently ensured that project milestones were achieved in a timely manner, contributing to the smooth progression of the thesis.</p>	

Technical level	A - excellent.
<i>Assess level of thesis specialty, use of knowledge gained by study and by expert literature, use of sources and data gained by</i>	

experience.

The thesis is technically sound, showcasing the student's adept handling of a challenging problem with a well-rounded and effective solution. The student has demonstrated commendable expertise across several relevant domains, including software development, machine learning, system operations and network security. This multidisciplinary proficiency is crucial given the technical complexity and the innovative nature of the project, which involves using state-of-the-art technology. Moreover, the student's use of a diverse set of tools reflects a strong, practical understanding of the technologies and methodologies pertinent to their field of study. This not only highlights their technical skills but also their ability to creatively apply these tools in a cohesive and effective manner.

Formal and language level, scope of thesis

B - very good.

Assess correctness of usage of formal notation. Assess typographical and language arrangement of thesis.

In general, the thesis is informative and clear. The student expressed in a correct language the different aspects involved in the process of building a LLM honeypot system using formal notation when required.

Selection of sources, citation correctness

A - excellent.

Present your opinion to student's activity when obtaining and using study materials for thesis creation. Characterize selection of sources. Assess that student used all relevant sources. Verify that all used elements are correctly distinguished from own results and thoughts. Assess that citation ethics has not been breached and that all bibliographic citations are complete and in accordance with citation convention and standards.

The student has always made reference to third party articles and software applications used for meeting the thesis assignment. In general, all references used in the work followed the proper quality standards

Additional commentary and evaluation

Present your opinion to achieved primary goals of thesis, e.g. level of theoretical results, level and functionality of technical or software conception, publication performance, experimental dexterity etc.

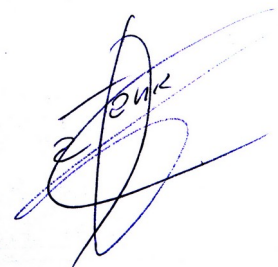
Please insert your commentary (voluntary evaluation).

III. OVERALL EVALUATION, QUESTIONS FOR DEFENSE, CLASSIFICATION SUGGESTION

Summarize thesis aspects that swayed your final evaluation.

In this thesis, the student has proposed a new method for the generation of honeypots using Large Language Models (LLM), with the aim of mimicking several protocols and improving the engagement of the intruders. The system features a specialized LLM, fine-tuned with tailored prompts for honeypots, and introduces new evaluation methods, including unit tests for LLMs and an LLM-based attacker model. Evaluation is conducted through two major experiments: one assessing generative capabilities with human participants and unit tests, and the other evaluating deceptive effectiveness with human participants in simulated attack scenarios. These experiments provide valuable insights into the system's performance.

I evaluate handed thesis with classification grade A - excellent.



Date: 06-13-2024

Signature: Carlos A. Catania