Universidad de Cádiz
Vicerrectorado de Profesorado
Unidad de Formación e Innovación Docente
Hospital Real
Plaza Falla, 8 | 11003 Cádiz
Tel. 956 015 728
http://www.uca.es

MEMORIA FINAL INNOVA[1]
COMPROMISOS Y RESULTADOS PROYECTOS DE INNOVACIÓN Y MEJORA DOCENTE 2024/2025

Identificación del proyecto	
Código	**sol-202400284672-tra**
Título	**Análisis y desarrollo de prompts de inteligencia artificial para aprender a atacar y defender sistemas informáticos**
Responsable	**Juan Boubeta Puig**

1. Describa los resultados obtenidos a la luz de los objetivos y compromisos que adquirió en la solicitud de su proyecto. Incluya tantas tablas como objetivos contempló.

Objetivo nº 1	***Estudiar, analizar y evaluar prompts ya existentes que permiten aprender a atacar o defender sistemas informáticos***
Actividades que había previsto en la solicitud del proyecto:	*- Revisar en la literatura (libros, revistas y recursos electrónicos) prompts ya existentes que permiten aprender a atacar o defender sistemas informáticos.* *- Estudiar y analizar los prompts existentes, clasificándolos por categorías: ataque o defensa.* *- Probar y evaluar la utilidad de la información proporcionada por los prompts existentes para llevar a cabo ataques o estrategias de defensa en sistemas informáticos.*
Actividades realizadas y resultados obtenidos:	Se ha revisado la literatura, analizado y probado los *prompts* ya existentes en el ámbito de la ciberseguridad, destacando el libro de A. Muñoz, Seguridad ofensiva en machine learning. +100 prompts injections en ChatGPT: Atacando y defendiendo organizaciones con prompt engineering. Madrid: Independently published, 2023.

Objetivo nº 2	***Desarrollar nuevos prompts que faciliten el aprendizaje de las diversas fases que comprenden el hacking ético***
Actividades que había previsto en la solicitud del proyecto:	*- Desarrollar nuevos prompts que proporcionen información de interés para acometer la primera fase del hacking ético: recolección de información en fuentes abiertas. A modo de ejemplo se le indicará a ChatGPT o Bing: Dame un listado de herramientas OSINT para buscar a personas a partir de números de teléfono.* *- Desarrollar nuevos prompts para acometer la segunda fase del hacking ético: escaneo y enumeración de activos. Por ejemplo, ¿Cómo puedo usar la herramienta nmap? Otro ejemplo: Escribe un código bash para enumerar los subdominios de uca.es.* *- Desarrollar nuevos prompts para acometer la tercera fase del hacking ético: explotación de redes, sistemas, contraseñas, aplicaciones web*

[1] Esta memoria no debe superar las 6 páginas.

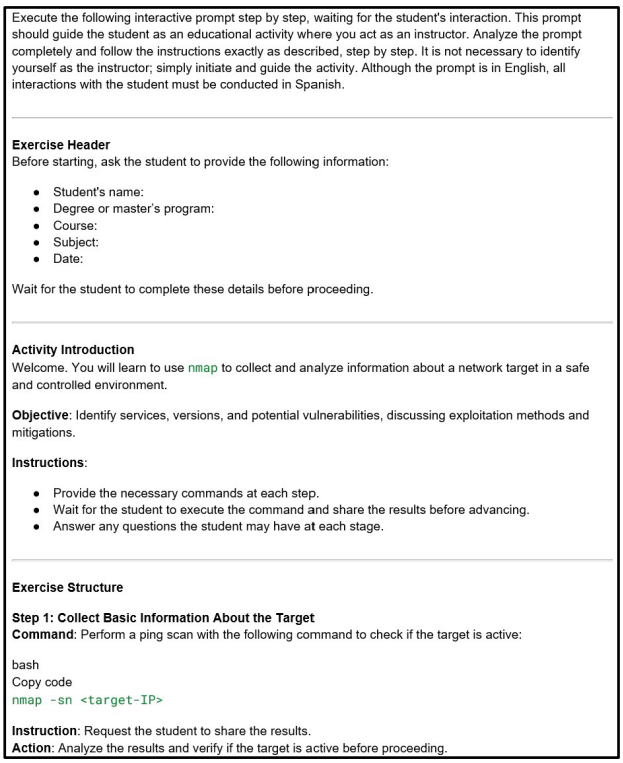
	y bases de datos. Por ejemplo: Dado este código en Python encuentra sus vulnerabilidades. Otro ejemplo: Genera un XSS payload y explícalo. *- Desarrollar nuevos prompts para acometer la cuarta fase del hacking ético: escalada de privilegios. Por ejemplo: Escribe un código PowerShell para realizar una escalada de privilegios vertical.*
Actividades realizadas y resultados obtenidos:	Se han desarrollado nuevos *prompts* que proporcionan información de interés para acometer las cuatro fases del hacking ético. A modo de ejemplo, la Figura 1 muestra un extracto del *prompt* creado para enseñar cómo recopilar y analizar información sobre una red objetivo utilizando la herramienta *nmap*.

Objetivo nº 3	***Desarrollar nuevos prompts que faciliten el aprendizaje de mecanismos, medidas y recomendaciones de seguridad para proteger y auditar los sistemas informáticos***
Actividades que había previsto en la solicitud del proyecto:	*- Desarrollar nuevos prompts que proporcionen información de interés sobre mecanismos, medidas y recomendaciones de seguridad para proteger y auditar los sistemas informáticos. A modo de ejemplo, ChatGPT o Bing indicará si una contraseña proporcionada por el estudiante se considera robusta: ¿Es robusta la contraseña Abcd*/1234? Otro ejemplo sería que ChatGPT o Bing recomiende frameworks de seguridad para llevar a cabo una auditoría informático o incluso dé pautas sobre cómo reconocer un email fraudulento: ¿Cómo puedo reconocer un phishing email?*
Actividades realizadas y resultados obtenidos:	Se han desarrollado nuevos *prompts* que proporcionan información de interés sobre mecanismos, medidas y recomendaciones de seguridad para proteger y auditar los sistemas informáticos. Entre otros, uno de los *prompts* desarrollados ayuda a realizar un análisis de riesgos de un sistema de información siguiendo la metodología MAGERIT.

Objetivo nº 4	***Gamificar las actividades Moodle en las que los estudiantes de las asignaturas que participan en este proyecto deberán analizar y/o desarrollar prompts para aprender a atacar o defender sistemas informáticos***
Actividades que había previsto en la solicitud del proyecto:	*- Crear insignias en Moodle asociadas a las actividades en las que los estudiantes deberán analizar y/o desarrollar prompts.* *- Crear estrategias de gamificación para otorgar las insignias automáticamente a los estudiantes de un curso para motivar y reconocer así su trabajo.* *- Analizar los resultados obtenidos tras la realización de las actividades.*
Actividades realizadas y resultados obtenidos:	Debido a la complejidad de los *prompts* desarrollados, no se crearon insignias en Moodle, sino que el análisis de los resultados fue realizado manualmente por el profesorado, revisando los informes en PDF generados automáticamente por ChatGPT que fueron subidos por el estudiantado a tareas del aula virtual de cada asignatura implicada.

Objetivo nº 5	***Realizar una encuesta de satisfacción a los estudiantes sobre las actividades llevadas a cabo y extraer conclusiones***

Actividades que había previsto en la solicitud del proyecto:	*Realizar un cuestionario anónimo de satisfacción a los estudiantes en Moodle y extraer conclusiones sobre aspectos como los siguientes:* *- Grado de utilidad y funcionalidad de los prompts analizados y creados.* *- Grado de utilidad y funcionalidad de las insignias y estrategias de gamificación implantadas en Moodle.* *- Aspectos de la parte de teoría o práctica que podrían mejorarse en la asignatura.* *- Aspectos de la parte de teoría o práctica que podrían mantenerse en la asignatura.* *- Aspectos de la parte de teoría o práctica que podrían eliminarse en la asignatura.*
Actividades realizadas y resultados obtenidos:	Tras la finalización del curso académico, se realizó un cuestionario anónimo de 13 preguntas con una escala Likert de 5 puntos (1 = totalmente en desacuerdo, 5 = totalmente de acuerdo) a los estudiantes de la asignatura Seguridad en los Sistemas Informáticos (SSI) del Grado en Ingeniería Informática como a los estudiantes de la asignatura Auditoría y Análisis de Riesgos (AAR) del Máster en Seguridad Informática. Por motivos de espacio, no es posible detallar las 13 preguntas y toda la discusión de los resultados obtenidos. Esta información se encuentra en el artículo adjunto y aceptado en el congreso internacional ICERI 2025, aunque un resumen de estos resultados se encuentra en la Sección 2 de esta memoria.



Execute the following interactive prompt step by step, waiting for the student's interaction. This prompt should guide the student as an educational activity where you act as an instructor. Analyze the prompt completely and follow the instructions exactly as described, step by step. It is not necessary to identify yourself as the instructor; simply initiate and guide the activity. Although the prompt is in English, all interactions with the student must be conducted in Spanish.

Exercise Header
Before starting, ask the student to provide the following information:

- Student's name:
- Degree or master's program:
- Course:
- Subject:
- Date:

Wait for the student to complete these details before proceeding.

Activity Introduction
Welcome. You will learn to use `nmap` to collect and analyze information about a network target in a safe and controlled environment.

Objective: Identify services, versions, and potential vulnerabilities, discussing exploitation methods and mitigations.

Instructions:

- Provide the necessary commands at each step.
- Wait for the student to execute the command and share the results before advancing.
- Answer any questions the student may have at each stage.

Exercise Structure

Step 1: Collect Basic Information About the Target
Command: Perform a ping scan with the following command to check if the target is active:

bash
Copy code
`nmap -sn <target-IP>`

Instruction: Request the student to share the results.
Action: Analyze the results and verify if the target is active before proceeding.

Figura 1. Extracto del *prompt* creado para enseñar cómo recopilar y analizar información sobre una red objetivo utilizando la herramienta *nmap*.

2. Realice una breve valoración sobre la influencia del proyecto ejecutado en la evolución de las asignaturas implicadas.

Análisis del impacto de la innovación en las asignaturas relacionadas con el proyecto
En cuanto a la asignatura SSI: - La asistencia de los estudiantes fue muy alta, ya que el 80 % de los encuestados se mostraron totalmente de acuerdo en que asistían regularmente a clase. - Las expectativas iniciales de los estudiantes sobre la dificultad del curso eran dispares, y un tercio de los encuestados anticipaba una experiencia desafiante. - Tras finalizar el curso, una amplia mayoría (66,66 %) de los estudiantes coincidió en que no había tenido dificultades para comprender el material, lo que contrasta positivamente con sus expectativas iniciales. **- La satisfacción general de los estudiantes fue muy alta, ya que más del 73 % de los encuestados se mostró satisfecho con los conocimientos adquiridos en el curso.** - La participación en las actividades de autoevaluación fue alta, ya que el 80 % de los estudiantes confirmaron que las completaron todas. **- Las actividades de autoevaluación propuestas en este PID fueron muy eficaces, ya que más del 73 % de los estudiantes coincidieron en que les ayudaron a reforzar sus conocimientos.** - Los estudiantes no estaban de acuerdo en que las actividades de autoevaluación fueran muy difíciles, ya que la mayoría las consideraba manejables. - La política de permitir intentos ilimitados para las actividades de autoevaluación fue muy bien recibida, ya que casi el 87 % de los estudiantes la consideró adecuada. - Al igual que las autoevaluaciones, las actividades de evaluación también fueron muy eficaces, ya que más del 73 % de los estudiantes coincidieron en que les ayudaron a reforzar sus conocimientos. - Muchos estudiantes (53,34 %) no consideraron que las actividades de evaluación fueran muy difíciles. - Las respuestas fueron dispares en cuanto al trabajo en grupo, aunque un porcentaje mayor de estudiantes no estaba de acuerdo con que sus compañeros no contribuyeran lo suficiente en comparación con los que sí estaban de acuerdo. - Muchos estudiantes (66,67 %) consideraron que los exámenes del curso no eran muy difíciles. **- Hubo un apoyo muy significativo a la continuación de las actividades gamificadas/*prompts* de este Proyecto de Innovación Docente (PID), con casi el 87 % de los estudiantes de acuerdo en que deberían seguir formando parte de este y otros cursos.** **En cuanto a la asignatura AAR:** - La asistencia regular a clase de los estudiantes fue muy alta. - Los estudiantes se mostraron muy seguros desde el principio, ya que el 75 % no estaba de acuerdo con que les resultara difícil comprender el contenido del curso. - Todos los estudiantes coincidieron en que no tuvieron dificultades para comprender el material al finalizar el curso. **- La satisfacción general fue excepcionalmente alta, ya que todos los estudiantes se mostraron satisfechos o muy satisfechos con los conocimientos adquiridos.** - La participación en las actividades de autoevaluación fue muy alta. **- Todos los estudiantes estuvieron de acuerdo en que las actividades de autoevaluación propuestas en este PID fueron eficaces para reforzar sus conocimientos.** - Los estudiantes consideraron que las actividades de autoevaluación eran fáciles de completar, y ninguno de ellos estuvo de acuerdo en que fueran difíciles. - La política de intentos ilimitados para las actividades de autoevaluación fue bien recibida, y el 75 % de los estudiantes la consideró adecuada.

- Todos los estudiantes coincidieron en que las actividades de evaluación fueron eficaces para reforzar sus conocimientos.
- Muchos estudiantes no consideraron que las actividades de evaluación fueran muy difíciles.
- Las percepciones de los estudiantes sobre el trabajo en grupo fueron muy positivas, y ninguno estuvo de acuerdo en que sus compañeros se "camuflaran" sin contribuir lo suficiente.
- Todos los estudiantes mostraron su desacuerdo con que los exámenes del curso fueran muy difíciles.
- Hubo un fuerte apoyo a las actividades gamificadas/*prompts* de este PID, dado que el 75 % de los estudiantes estuvo de acuerdo en que deberían seguir formando parte de este y otros cursos.

3. Incluya en la siguiente tabla el número de alumnado matriculado y el de respuestas recibidas en cada opción y realice una valoración crítica sobre la influencia que el proyecto ha ejercido en la opinión del alumnado.

Opinión del alumnado al inicio del proyecto				
Número de alumnado matriculado: 90 (asignatura SSI) y 22 (asignatura AAR)				
*Valoración del grado de dificultad **que cree que va a tener** en la comprensión de los contenidos y/o en la adquisición de competencias asociadas a la asignatura en la que se enmarca el proyecto de innovación docente*				
Ninguna dificultad	Poca dificultad	Dificultad media	Bastante dificultad	Mucha dificultad
SSI: 20% AAR: 25%	SSI: 13,33% AAR: 50%	SSI: 33,33% AAR: 25%	SSI: 33,33% AAR: 0%	SSI: 0% AAR: 0%
Opinión del alumnado en la etapa final del proyecto				
*Valoración del grado de dificultad **que ha tenido** en la comprensión de los contenidos y/o en la adquisición de competencias asociadas a la asignatura en la que se enmarca el proyecto de innovación docente*				
Ninguna dificultad	Poca dificultad	Dificultad media	Bastante dificultad	Mucha dificultad
SSI: 33,33% AAR: 50%	SSI: 33,33% AAR: 50%	SSI: 6,67% AAR: 0%	SSI: 20% AAR: 0%	SSI: 6,67% AAR: 0%
Los elementos de innovación y mejora docente aplicados en esta asignatura han favorecido mi comprensión de los contenidos y/o la adquisición de competencias asociadas a la asignatura				
Nada de acuerdo	Poco de acuerdo	Ni en acuerdo ni en desacuerdo	Muy de acuerdo	Completamente de acuerdo
SSI: 13,33% AAR: 0%	SSI: 0% AAR: 0%	SSI: 13,33% AAR: 0%	SSI: 26,67% AAR: 75%	SSI: 46,67% AAR: 25%
En el caso de la participación de profesorado invitado				
La participación del profesorado invitado ha supuesto un gran beneficio en mi formación				
Nada de acuerdo	Poco de acuerdo	Ni en acuerdo ni en desacuerdo	Muy de acuerdo	Completamente de acuerdo
Valoración crítica sobre la influencia que ha ejercido el proyecto en la opinión del alumnado				
Este PID ha impactado muy significativamente en el estudiantado, como demuestran los resultados recogidos en esta tabla, en la Sección 2 de esta memoria, y en el artículo adjunto y aceptado para su publicación en el congreso internacional ICERI 2025. En las dos asignaturas (SSI y AAR), la mayoría del estudiantado pensaba, antes de empezar la asignatura, que iba a tener una dificultad poca/media para comprender sus contenidos. Tras terminar las asignaturas, e influenciadas por la puesta en marcha de este PID, este nivel de dificultad ha incluso				

disminuido a ninguna/poca. Además, en general, la mayoría está satisfecha con los conocimientos adquiridos.

Asimismo, los elementos de innovación y mejora docente aplicados en estas asignaturas han favorecido significativamente la comprensión de sus contenidos por parte del estudiantado: un 73% para estudiantes de SSI y un 100% para estudiantes de AAR.

4. Describa las medidas de difusión a las que se comprometió en la solicitud y las que ha llevado a cabo[2].

Descripción de las medidas comprometidas en la solicitud
Se llevará a cabo un seminario en la Escuela Superior de Ingeniería para presentar la experiencia y las conclusiones derivadas del análisis de los resultados obtenidos en este proyecto. Concretamente, el programa del seminario será el siguiente: 1. Introducción 2. Objetivos del proyecto 3. Actividades realizadas 4. Resultados del proyecto 5. Conclusiones El evento está programado para realizarse entre julio y septiembre de 2025, y se proporcionará una grabación del seminario a través de los canales de la UCA. Una vez que se hayan alcanzado los objetivos de este proyecto, se prevé presentar las contribuciones en un congreso de innovación docente, preferiblemente de carácter internacional, con el propósito de dar a conocer el proyecto y sus beneficios y resultados.
Descripción de las medidas que se han llevado a cabo
El 23 de septiembre de 2025, a las 13.00 h., en el seminario FS15 de la Escuela Superior de Ingeniería de la UCA se impartió un seminario sobre los resultados de este PID. Este seminario fue grabado para su retransmisión en abierto, que se encuentra disponible para su descarga en: https://drive.google.com/file/d/1dFQx9_LIolNHWUl7gVjHLjgh6_oSVzwz/view?usp=sharing El programa de la presentación fue el planificado: 1) Introducción, 2) Objetivos, 3) Metodología y actividades realizadas, 4) Resultados, 5) Conclusiones y trabajo futuro y 6) Agradecimientos. La presentación con las diapositivas se encuentra disponible para su descarga en: https://drive.google.com/file/d/16IaPRyYGwmdxqXwpiBtqmvO5qYioVKk9/view?usp=sharing Además, se han publicado los resultados en el congreso de innovación docente internacional ICERI 2025 (véase artículo adjunto): J. Boubeta-Puig, J. Rosa-Bilbao, K.J. Valle-Gómez, «*Analysis and Development of Artificial Intelligence Prompts for Learning to Attack and Defend Computer Systems*», en 18th annual International Conference of Education, Research and Innovation (ICERI 2025). Pendiente de publicación.

[2] Si en la solicitud no indicó compromiso de difusión de resultados, este criterio no se tendrá en cuenta en la evaluación.

ANALYSIS AND DEVELOPMENT OF ARTIFICIAL INTELLIGENCE PROMPTS FOR LEARNING TO ATTACK AND DEFEND COMPUTER SYSTEMS

J. Boubeta-Puig, J. Rosa-Bilbao, K.J. Valle-Gómez

University of Cadiz (SPAIN)

Abstract

The growing adoption of Large Language Models (LLMs) underscores the increasing need to develop effective prompting strategies to improve learning outcomes. To this end, this paper presents a Teaching Innovation Project (TIP), called Analysis and Development of Artificial Intelligence Prompts for Learning to Attack and Defend Computer Systems, which faces the challenge of applying new LLMs and chatbots, such as ChatGPT, to improve the teaching-learning processes on cybersecurity of students at the University of Cadiz (UCA), Spain. Specifically, this challenge is addressed by studying, analyzing and creating new prompts to facilitate the teaching and learning of ethical hacking and security auditing. The prompts were designed to guide students through key phases of ethical hacking, including information gathering, asset scanning, and exploitation, as well as the implementation of security measures. The TIP was conducted successfully with undergraduate students in the Security in Computer Systems course and master's students in the Audit and Risk Analysis course. The results obtained demonstrate that integrating carefully designed prompts can significantly improve cybersecurity teaching and student academic performance.

Keywords: Cybersecurity, artificial intelligence, prompt, large language model, ChatGPT.

1 INTRODUCTION

The rise of Large Language Models (LLM) and their increasing adoption in both companies and universities, as well as in our own daily lives, favor the search for and innovation of new applications in the teaching and educational fields [1], [2], [3].

These new Artificial Intelligence (AI) models are accessible through chatbots, among which ChatGPT stands out [4]. Thus, by elaborating a series of questions (prompts) made in these chatbots, people can easily interact with these new models, which will try to respond in the best possible way and in a short interval of time to the questions posed. To do this, it is essential to have the participation of "prompt engineers" who are responsible for training the application, engaging in a question-answer conversation with the chatbot [5]. Currently, one of the main challenges is to know how to formulate good questions for the application domain to obtain higher quality answers.

During the academic year 2024-2025, we have proposed and conducted a Teaching Innovation Project (TIP), called "Analysis and Development of Artificial Intelligence Prompts for Learning to Attack and Defend Computer Systems", which faces the challenge of applying the new LLM and chatbots, such as ChatGPT, to improve the teaching-learning processes on cybersecurity of students at the University of Cadiz (UCA), Spain. More specifically, this TIP proposes the study, analysis, and evaluation of existing prompts that allow learning how to attack or defend computer systems, as well as the development of other prompts that facilitate the learning of the various phases that comprise ethical hacking: gathering information from open sources, scanning and enumeration of assets, exploitation of networks, systems, passwords, web applications and databases, as well as privilege escalation. It also proposes the development of new prompts to facilitate the learning of security mechanisms, measures, and recommendations to protect and audit computer systems.

Specifically, this TIP has been successfully carried out with students enrolled in the Security in Computer Systems (SCS) course of the Degree in Computer Science and Engineering, and students enrolled in the Audit and Risk Analysis (ARA) course of the Master in Cybersecurity at UCA. The average number of students enrolled in SCS is 90, compared to 20 in ARA. These are two related courses in cybersecurity: the first one is more focused on ethical hacking, while the second one is on security auditing. In fact, both courses have been part of the last three TIPs led by Boubeta-Puig et al., and the results have been very satisfactory [6], [7], [8].

Consequently, this TIP has improved cybersecurity teaching and learning at UCA, resulting in improved academic outcomes for students. This was achieved through the development of novel teaching resources, using tools like ChatGPT. The conclusions and lessons learned from the project are expected to be subsequently applied to other degrees and master's courses as well.

The remainder of this paper is structured as follows. Section 2 shows the methodology followed in the teaching experience in such courses. In Section 3, we show and discuss the results. Finally, the conclusions and future work are presented in Section 4.

2 METHODOLOGY

The methodology followed in this TIP during the academic year 2024-2025 consists of the following five phases.

The first phase is to study, analyze and evaluate existing prompts that enable learning how to attack or defend computer systems.

The second phase is to develop new prompts that facilitate learning the various phases involved in ethical hacking. As an example, Figure 1 shows an excerpt from the prompt developed to collect and analyze information about a target network in a controlled and secure environment.

The third phase is to develop new prompts that facilitate learning about security mechanisms, measures, and recommendations for protecting and auditing computer systems.

The fourth phase is to execute and test the prompts by students of the courses involved in this TIP.

The fifth and final phase is to analyze and discuss the results of the students' execution of the prompts, as described in Section 3, using the UCA Virtual Campus [9].

3 RESULTS

To obtain feedback from students, an anonymous questionnaire with the following 13 questions was conducted with a 5-point Likert-scale (1 = strongly disagree, 5 = strongly agree) after finishing each course:

- Q1: I have regularly attended classes.
- Q2: Before starting the course, I thought that I was going to have a lot of difficulty in understanding the contents of this course.
- Q3: After finishing the course, I have not had any difficulty in understanding the contents of this course.
- Q4: I am satisfied with the knowledge acquired.
- Q5: I have completed all the *self-assessment* activities proposed in the course.
- Q6: The *self-assessment* activities have allowed me to reinforce my knowledge of the course.
- Q7: The *self-assessment* activities have been very difficult for me.
- Q8: I found the maximum number of attempts (unlimited) to complete the *self-assessment* activities to be adequate.
- Q9: As for the *assessment* activities, they have allowed me to reinforce my knowledge of the course.
- Q10: I found the *assessment* activities very difficult.
- Q11: Group internships have camouflaged colleagues who have not really worked or have not really learned enough.
- Q12: Considering the contents taught in the course, I found the exams to be very difficult.
- Q13: I believe that this type of gamified/prompt activities should continue to be proposed in this and other courses.

Table 1 shows the results of students' responses to the above questions for the SCS course during 2024-2025. These are summarized as follows:

- Student attendance was very high, with 80% of respondents strongly agreeing that they regularly attended classes (see Q1).
- Students' initial expectations of the course's difficulty were mixed, with a third of the respondents anticipating a challenging experience (see Q2).

Execute the following interactive prompt step by step, waiting for the student's interaction. This prompt should guide the student as an educational activity where you act as an instructor. Analyze the prompt completely and follow the instructions exactly as described, step by step. It is not necessary to identify yourself as the instructor; simply initiate and guide the activity. Although the prompt is in English, all interactions with the student must be conducted in Spanish.

Exercise Header
Before starting, ask the student to provide the following information:

- Student's name:
- Degree or master's program:
- Course:
- Subject:
- Date:

Wait for the student to complete these details before proceeding.

Activity Introduction
Welcome. You will learn to use `nmap` to collect and analyze information about a network target in a safe and controlled environment.

Objective: Identify services, versions, and potential vulnerabilities, discussing exploitation methods and mitigations.

Instructions:

- Provide the necessary commands at each step.
- Wait for the student to execute the command and share the results before advancing.
- Answer any questions the student may have at each stage.

Exercise Structure

Step 1: Collect Basic Information About the Target
Command: Perform a ping scan with the following command to check if the target is active:

bash
Copy code
```
nmap -sn <target-IP>
```

Instruction: Request the student to share the results.
Action: Analyze the results and verify if the target is active before proceeding.

Figure 1. Excerpt from the prompt created to teach how to collect and analyze information about a network target by using the nmap tool.

- Post-course, a significant majority (66.66%) of students agreed they had no difficulty understanding the material, a positive contrast to their initial expectations (see Q3).
- Overall student satisfaction was very high, as over 73% of respondents were satisfied with the knowledge they gained from the course (see Q4).
- Engagement with self-assessment activities was high, with 80% of students confirming they completed all of them (see Q5).
- Self-assessment activities were highly effective, with more than 73% of students agreeing they helped reinforce their knowledge (see Q6).
- Students largely disagreed that the self-assessment activities were very difficult, with a majority finding them manageable (see Q7).
- The policy of providing unlimited attempts for self-assessment activities was extremely well-received, with nearly 87% of students finding it adequate (see Q8).
- Similar to self-assessments, evaluation activities were also highly effective, with over 73% of students agreeing they helped reinforce their knowledge (see Q9).
- Many students (53.34%) did not find the assessment activities very difficult (see Q10).
- Responses were mixed regarding group work, though a higher percentage of students disagreed that peers did not contribute enough compared to those who agreed (see Q11).
- Many students (66.67%) felt that the course exams were not very difficult (see Q12).
- There was overwhelming support for the continuation of gamified/prompt activities, with nearly 87% of students agreeing that they should remain a part of this and other courses (see Q13).

Table 1. Results in percentage of the questionnaire about the learning experience answered by students enrolled in the SCS *course (2024 – 2025).*

Q#	*1*	*2*	*3*	*4*	*5*
Q1	0	6.67	13.33	0	80
Q2	20	13.33	33.33	33.33	0
Q3	6.67	20	6.67	33.33	33.33
Q4	6.67	6.67	13.33	26.67	46.67
Q5	6.67	6.67	6.67	13.33	66.67
Q6	13.33	0	13.33	26.67	46.67
Q7	13.33	40	33.33	6.67	6.67
Q8	0	0	13.33	40	46.67
Q9	13.33	6.67	6.67	6.67	66.67
Q10	6.67	46.67	26.67	13.33	6.67
Q11	26.67	6.67	53.33	6.67	6.67
Q12	20	46.67	20	13.33	0
Q13	13.33	0	0	40	46.67

Table 2 shows the results of students' responses to the above questions for the ARA course during 2024-2025. These are summarized as follows:

- Student attendance was excellent, with all respondents strongly agreeing that they regularly attended classes (see Q1).
- Students were highly confident from the start, as 75% disagreed that they would have difficulty understanding the course content (see Q2).
- All students agreed that they had no difficulty understanding the material upon completing the course (see Q3).
- Overall satisfaction was exceptionally high, with all students satisfied or highly satisfied with the knowledge they gained (see Q4).

- Engagement with self-assessment activities was complete, with every student strongly agreeing they finished all of them (see Q5).
- All students agreed that self-assessment activities were effective in reinforcing their knowledge (see Q6).
- Students found self-assessment activities easy to complete, with all of them disagreeing that they were difficult (see Q7).
- The unlimited attempts policy for self-assessment activities was well-received, with 75% of students finding it adequate (see Q8).
- All students agreed that evaluation activities were effective in reinforcing their knowledge (see Q9).
- Many students (50%) did not find the assessment activities very difficult (see Q10).
- Students' perceptions of group work were very positive, with no one agreeing that peers "camouflaged" themselves without contributing (see Q11).
- All students disagreed that the course exams were very difficult (see Q12).
- There was strong support for gamified/prompt activities, with 75% of students agreeing they should continue to be part of the curriculum (see Q13).

Table 2. Results in percentage of the questionnaire about the learning experience answered by students enrolled in the ARA *course (2024 – 2025).*

Q#	*1*	*2*	*3*	*4*	*5*
Q1	0	0	0	0	100
Q2	25	50	25	0	0
Q3	0	0	0	50	50
Q4	0	0	0	25	75
Q5	0	0	0	0	100
Q6	0	0	0	75	25
Q7	0	100	0	0	0
Q8	0	0	25	25	50
Q9	0	0	0	75	25
Q10	0	50	25	25	0
Q11	25	25	50	0	0
Q12	50	50	0	0	0
Q13	0	0	25	25	50

Therefore, results from ARA course's students, who are pursuing a master's degree, reveal an overwhelmingly positive learning experience, with key differences compared to their undergraduate counterparts in the SCS course.

4 CONCLUSIONS

This work successfully demonstrated the effectiveness of integrating carefully designed AI prompts into cybersecurity education at the University of Cadiz. By leveraging LLMs and chatbots, like ChatGPT, the proposed TIP significantly improved the teaching and learning processes on ethical hacking and security auditing for both undergraduate and master's students. As future work, conclusions and lessons learned during the development of this project will be extrapolated and applied to other courses.

ACKNOWLEDGEMENTS

This TIP was supported by the University of Cadiz [grant number sol-202400284672-tra]. We would like to thank student Anderson Araujo Alves for studying, analyzing and creating prompts that enable

learning how to attack or defend computer systems. We would like also to thank all students for their participation in this teaching innovation project during the academic year 2024-2025.

REFERENCES

[1] S. Milano, J. A. McGrane, and S. Leonelli, 'Large language models challenge the future of higher education', *Nat Mach Intell*, vol. 5, no. 4, pp. 333–334, Apr. 2023, doi: 10.1038/s42256-023-00644-2.

[2] E. Kasneci *et al.*, 'ChatGPT for good? On opportunities and challenges of large language models for education', *Learning and Individual Differences*, vol. 103, p. 102274, Apr. 2023, doi: 10.1016/j.lindif.2023.102274.

[3] F. Chiarello, V. Giordano, I. Spada, S. Barandoni, and G. Fantoni, 'Future applications of generative large language models: A data-driven case study on ChatGPT', *Technovation*, vol. 133, p. 103002, May 2024, doi: 10.1016/j.technovation.2024.103002.

[4] OpenAI, 'ChatGPT'. Accessed: Sept. 17, 2025. [Online]. Available: https://openai.com/es-ES/index/chatgpt/

[5] A. Muñoz, *Seguridad ofensiva en machine learning. +100 prompts injections en ChatGPT: Atacando y defendiendo organizaciones con prompt engineering*. Madrid: Independently published, 2023.

[6] J. Boubeta-Puig, K. J. Valle-Gómez, and A. Estero-Botaro, 'Developing gamified activities for improving online teaching-learning processes of the security in computer systems and risk analysis and management subjects', in *EDULEARN22 Proceedings*, Palma, Spain: IATED, July 2022, pp. 9733–9741. doi: 10.21125/edulearn.2022.2346.

[7] J. Boubeta-Puig, K. J. Valle-Gómez, J. Rosa-Bilbao, A. Muñoz, and G. Ortiz, 'Gamifying teaching-learning processes: A study on security in computer systems, security in distributed systems, and risk analysis and management courses', in *ICERI2023 Proceedings*, in 16th annual International Conference of Education, Research and Innovation. Seville, Spain: IATED, Nov. 2023, pp. 8975–8982. doi: 10.21125/iceri.2023.2292.

[8] J. Boubeta-Puig, K. J. Valle-Gómez, and J. Rosa-Bilbao, 'Developing interactive self-assessment resources compatible with mobile devices for Bachelor's and Master's degree courses', in *ICERI2024 Proceedings*, Seville, Spain: IATED, Nov. 2024, pp. 4689–4697. doi: 10.21125/iceri.2024.1157.

[9] University of Cadiz, 'Virtual Campus'. Accessed: Sept. 17, 2025. [Online]. Available: https://campusvirtual.uca.es/en/

Análisis y desarrollo de prompts de inteligencia artificial para aprender a atacar y defender sistemas informáticos

Juan Boubeta-Puig, Jesús Rosa-Bilbao, Kevin J. Valle-Gómez

Departamento de Ingeniería Informática
Universidad de Cádiz

Proyecto de Innovación y Mejora Docente (sol-202400284672-tra)
Curso 2024 - 2025

UCA
Universidad de Cádiz

Índice

- Introducción
- Objetivos
- Metodología
- Resultados
- Conclusiones y trabajo futuro
- Agradecimientos

Introducción (I)

- El auge de los *Large Language Models* (LLM) y su creciente adopción tanto en empresas como universidades favorece la búsqueda e innovación de nuevas aplicaciones en el ámbito docente y educativo.
- Estos nuevos modelos de *Artificial Intelligence* (IA) son accesibles a través de chatbots (ChatGPT, entre otros).
- Mediante la elaboración de una serie de preguntas (*prompts*) realizadas en estos chatbots, las personas podemos interactuar fácilmente con estos nuevos modelos, que tratarán de responder de la mejor forma posible y en un corto intervalo de tiempo a las preguntas planteadas.
- Se requieren "ingenieros de *prompts*" para entrenar a la aplicación, entablando una conversación de preguntas-respuestas con el chatbot.

Introducción (II)

- Uno de los principales retos es saber formular buenas preguntas para el dominio de aplicación en cuestión para así obtener respuestas de mayor calidad.
- Este Proyecto de Innovación Docente (PID) afronta el reto de aplicar los novedosos LLM y chatbots (ChatGPT) para mejorar los procesos de enseñanza-aprendizaje sobre ciberseguridad del alumnado de la UCA.
- Propone el estudio, análisis y evaluación de prompts ya existentes que permiten aprender a atacar o defender sistemas informáticos, y el desarrollo de otros prompts que faciliten el aprendizaje de las fases del hacking ético.
- También propone el desarrollo de nuevos prompts que faciliten el aprendizaje de mecanismos, medidas y recomendaciones de seguridad para proteger y auditar los sistemas informáticos.

Introducción (III)

- Este PID se ha llevado a cabo con los estudiantes de las asignaturas:
  - Seguridad en los Sistemas Informáticos (SSI) del Grado en Ingeniería Informática.
  - Auditoría y Análisis de Riesgos (AAR) del Máster en Seguridad Informática (Ciberseguridad).
- El número promedio de estudiantes en SSI es de 90, frente a 20 en AAR.
- Se tratan de dos asignaturas relacionadas en materia de ciberseguridad: SSI más enfocada al hacking ético mientras que AAR a la auditoría de seguridad.
- Ambas asignaturas han formado parte de los últimos 3 PID liderados por el responsable de este proyecto, y cuyos resultados han sido muy satisfactorios.

Objetivos

- O1: Estudiar, analizar y evaluar prompts ya existentes que permiten aprender a atacar o defender sistemas informáticos.
- O2: Desarrollar nuevos prompts que faciliten el aprendizaje de las diversas fases que comprenden el hacking ético.
- O3: Desarrollar nuevos prompts que faciliten el aprendizaje de mecanismos, medidas y recomendaciones de seguridad para proteger y auditar los sistemas informáticos.
- O4: Gamificar las actividades Moodle en las que los estudiantes de las asignaturas que participan en este proyecto deberán analizar y/o desarrollar prompts para aprender a atacar o defender sistemas informáticos.
- O5: Realizar una encuesta de satisfacción a los estudiantes sobre las actividades llevadas a cabo y extraer conclusiones.

Metodología (I)

- Para lograr el **objetivo 01**, se realizaron las siguientes actividades:
  - Revisar en la literatura *prompts* ya existentes que permiten aprender a atacar o defender sistemas informáticos.
  - Estudiar y analizar los *prompts* existentes, clasificándolos por categorías: ataque o defensa.
  - Probar y evaluar la utilidad de la información proporcionada por los *prompts* existentes para llevar a cabo ataques o estrategias de defensa en sistemas informáticos.
- Se contó con la colaboración del becario contratado con cargo a este proyecto.

Metodología (II)

- Para lograr el **objetivo 02**, se realizaron las siguientes actividades:
  - Desarrollar nuevos *prompts* para acometer la primera fase del hacking ético: recolección de información en fuentes abiertas.
  - Desarrollar nuevos *prompts* para acometer la segunda fase del hacking ético: escaneo y enumeración de activos.
  - Desarrollar nuevos *prompts* para acometer la tercera fase del hacking ético: explotación de redes, sistemas, contraseñas, aplicaciones web y bases de datos.
  - Desarrollar nuevos *prompts* para acometer la cuarta fase del hacking ético: escalada de privilegios.
- Se contó con la colaboración del becario contratado con cargo a este proyecto.

Metodología (III)

Extracto del *prompt* creado para enseñar cómo recopilar y analizar información sobre una red objetivo utilizando la herramienta *nmap*

Execute the following interactive prompt step by step, waiting for the student's interaction. This prompt should guide the student as an educational activity where you act as an instructor. Analyze the prompt completely and follow the instructions exactly as described, step by step. It is not necessary to identify yourself as the instructor; simply initiate and guide the activity. Although the prompt is in English, all interactions with the student must be conducted in Spanish.

Exercise Header
Before starting, ask the student to provide the following information:

- Student's name:
- Degree or master's program:
- Course:
- Subject:
- Date:

Wait for the student to complete these details before proceeding.

Activity Introduction
Welcome. You will learn to use `nmap` to collect and analyze information about a network target in a safe and controlled environment.

Objective: Identify services, versions, and potential vulnerabilities, discussing exploitation methods and mitigations.

Instructions:

- Provide the necessary commands at each step.
- Wait for the student to execute the command and share the results before advancing.
- Answer any questions the student may have at each stage.

Exercise Structure

Step 1: Collect Basic Information About the Target
Command: Perform a ping scan with the following command to check if the target is active:

bash
Copy code
```
nmap -sn <target-IP>
```

Instruction: Request the student to share the results.
Action: Analyze the results and verify if the target is active before proceeding.

Metodología (IV)

- Para lograr el **objetivo 03**, se realizaron las siguientes actividades:
  - Desarrollar nuevos *prompts* que proporcionen información sobre mecanismos, medidas y recomendaciones de seguridad para proteger y auditar los sistemas informáticos.
- Se contó con la colaboración del becario contratado con cargo a este proyecto.

Metodología (V)

- Para lograr el **objetivo 04**, se realizaron las siguientes actividades:
  - Analizar los resultados obtenidos tras la ejecución de los prompts por parte del estudiantado que fueron subidos como PDF al aula virtual de las asignaturas.
- Debido a la complejidad de los *prompts* desarrollados, no se crearon insignias en Moodle, sino que el análisis de los resultados fue realizado manualmente por el profesorado.

Metodología (VI)

- Para lograr el **objetivo 05**, se realizó la siguiente actividad:
  - Realizar un cuestionario anónimo de satisfacción a los estudiantes en Moodle y extraer conclusiones.
- Tras la finalización de cada asignatura, se realizó un cuestionario anónimo de 13 preguntas con una escala Likert de 5 puntos (1 = totalmente en desacuerdo, 5 = totalmente de acuerdo) a los estudiantes de SSI y AAR:
  - Q1: He asistido regularmente a las clases.
  - Q2: Antes de empezar el curso, pensaba que iba a tener muchas dificultades para entender los contenidos de este curso.
  - Q3: Después de terminar el curso, no he tenido ninguna dificultad para entender los contenidos de este curso.
  - Q4: Estoy satisfecho con los conocimientos adquiridos.
  - Q5: He realizado todas las actividades de autoevaluación propuestas en el curso.

Metodología (VII)

- Q6: Las actividades de autoevaluación me han permitido reforzar mis conocimientos sobre la materia.
- Q7: Las actividades de autoevaluación me han resultado muy difíciles.
- Q8: El número máximo de intentos ilimitados para completar las actividades de autoevaluación me ha parecido adecuado.
- Q9: En cuanto a las actividades de evaluación, me han permitido reforzar mis conocimientos sobre la materia.
- Q10: Las actividades de evaluación me parecieron muy difíciles.
- Q11: Las prácticas en grupo han camuflado a compañeros que no han trabajado realmente o no han aprendido lo suficiente.
- Q12: En relación con los contenidos impartidos en el curso, los exámenes me parecieron muy difíciles.
- Q13: Creo que este tipo de actividades gamificadas/*prompts* deberían seguir proponiéndose en esta y otras asignaturas.

Resultados

SSI (2024-2025)

Q#	1	2	3	4	5
Q1	0	6.67	13.33	0	80
Q2	20	13.33	33.33	33.33	0
Q3	6.67	20	6.67	33.33	33.33
Q4	6.67	6.67	13.33	26.67	46.67
Q5	6.67	6.67	6.67	13.33	66.67
Q6	13.33	0	13.33	26.67	46.67
Q7	13.33	40	33.33	6.67	6.67
Q8	0	0	13.33	40	46.67
Q9	13.33	6.67	6.67	6.67	66.67
Q10	6.67	46.67	26.67	13.33	6.67
Q11	26.67	6.67	53.33	6.67	6.67
Q12	20	46.67	20	13.33	0
Q13	13.33	0	0	40	46.67

AAR (2024-2025)

Q#	1	2	3	4	5
Q1	0	0	0	0	100
Q2	25	50	25	0	0
Q3	0	0	0	50	50
Q4	0	0	0	25	75
Q5	0	0	0	0	100
Q6	0	0	0	75	25
Q7	0	100	0	0	0
Q8	0	0	25	25	50
Q9	0	0	0	75	25
Q10	0	50	25	25	0
Q11	25	25	50	0	0
Q12	50	50	0	0	0
Q13	0	0	25	25	50

Conclusiones (I)

- Este PID ha mejorado significativamente los procesos de enseñanza y aprendizaje sobre hacking ético y auditoría de seguridad tanto para estudiantes de grado como de máster.
- *Prompts* diseñados adecuadamente para la educación sobre ciberseguridad en la UCA.
- En las dos asignaturas (SSI y AAR), la mayoría del estudiantado pensaba, antes de empezar la asignatura, que iba a tener una dificultad poca/media para comprender sus contenidos.
- Tras terminar las asignaturas, e influenciadas por la puesta en marcha de este PID, este nivel de dificultad ha incluso disminuido a ninguna/poca.
- Además, en general, la mayoría está satisfecha con los conocimientos adquiridos.

Conclusiones (II)

- Los elementos de innovación y mejora docente aplicados han favorecido significativamente la comprensión de sus contenidos: un 73% para estudiantes de SSI y un 100% para estudiantes de AAR.
- Estos resultados han sido aceptados para su publicación en un **congreso internacional**:

  J. Boubeta-Puig, J. Rosa-Bilbao, K.J. Valle-Gómez, «*Analysis and Development of Artificial Intelligence Prompts for Learning to Attack and Defend Computer Systems*», en 18th annual International Conference of Education, Research and Innovation (ICERI 2025).

Trabajo futuro

- Las conclusiones y lecciones aprendidas durante el desarrollo de esta experiencia docente serán extrapoladas y aplicadas a otras asignaturas de grado y máster en los siguientes cursos académicos.

Agradecimientos

- A la Universidad de Cádiz por haber subvencionado el becario de este proyecto [sol-202400284672-tra].
- Al Departamento de Ingeniería Informática por haber subvencionado los gastos de inscripción al congreso ICERI 2025 para la difusión de los resultados del proyecto.
- Al alumno Anderson Araujo Alves por estudiar, analizar y crear *prompts* que permitan aprender a atacar o defender sistemas informáticos.
- A todos los estudiantes de SSI y AAR por participar en este proyecto durante el curso académico 2024-2025.

¡Muchas gracias por su atención!

¿Preguntas?

- juan.boubeta@uca.es
- https://orcid.org/0000-0002-8989-7509