PentHack: AI-Enabled Penetration Testing Platform for Knowledge Development

Meera Alaryani, Shamsa Alremeithi, Fatima Al Ali and Richard Ikuesan
Zayed University, Abu Dhabi, United Arab Emirates

202102492@zu.ac.ae
202005474@zu.ac.ae
201915426@zu.ac.ae
Richard.ikuesan@zu.ac.ae

Abstract: The process of conducting and executing penetration testing within the pedagogical paradigm often requires complex and arduous processes. This is especially daunting for beginners who often struggle with the complexities of penetration processes: reconnaissance, enumeration, and system hacking. Research works to address this complexity leverage industry tools that have proven to work for industry-related training, however, they fail to support pedagogical learning in higher education systems. To address this limitation, this study proposed the development of an academic-focused penetration testing learning platform. The proposed approach integrates large language models (LLM) into the penetration testing lifecycle through a user-friendly GUI tool. The tool addresses the void in beginner-friendly ethical hacking tools by offering a stepwise guide, built-in commands and justifications, report generation, and an LLM prompt-engineered output displayed in a simple tabular format for easy reference. Furthermore, the tool provides an interactive menu for each phase of the penetration lifecycle thereby guiding users through common penetration testing commands. To cater to deeper learning needs, the tool leverages LLMs to furnish additional information on commands, empowering users with AI-generated insights. With the capability to compile a comprehensive report with all commands and logs acquired during its use, the proposed tool has the potential to reduce the time spent on research and decision-making. In addition, it streamlines the learning curve, allowing a more informed and structured approach to Pen-testing for beginners. By leveraging this platform, academics and learners can enhance their penetration testing knowledge without the complexities associated with learning penetration testing.

Keywords: Penetration Testing, Artificial Intelligence, Knowledge Development, Cyber Security Education, Pedagogy

1. Introduction

In the contemporary digital age, the Internet stands out as the linchpin that connects the threads of our technological progress. An omnipresent force creating our present, with origins in the late 1960s was a military project called ARPANET, which was built to withstand atomic attacks. Following that, in the late 1980s, the World Wide Web was launched, marking an important turning point in its transformative journey. Today, the Internet is a digital giant that cuts across numerous geographical boundaries, transforming social interactions, knowledge exchange, and global connectedness. Its impact on education, culture, and social dynamics has been nothing short of phenomenal, according to Castells (Castells, 2019; Navarria, 2016), who emphasized the Internet's role in building a more gregarious digital world. As we delve into the technical world, the Internet's evolution has become a tribute to human creativity, evolving from room-sized equipment to an era of pocket-sized handheld devices. The Internet's continual growth underlines its vital role in establishing an interconnected society in which information flows easily across borders, influencing the very fabric of our world. Graham and Dutton (2019) emphasized how software applications, vast databases, and interconnected network systems have brought the world together, facilitating fast connections. As well as maintaining vigilance in the face of technological advances is critical, underlining the need to embrace innovation and stay current with trends, as noted by Koutsikouri et al. (2018). Looking ahead, IT trends predict a future dominated by artificial intelligence (AI) and machine learning, which will transform job execution and decision-making processes across a variety of fields. This dynamic merging of the two drives information technology into new territory, transitioning from mainframes to the intricate interweaving of modern technologies (Duan, Edwards, & Dwivedi, 2019). As the force that drives growth, information technology continues to change the way people live, work, and perceive the world.

With the onset of the COVID-19 pandemic and the increased reliance on remote work and digital technologies, the attack surface has increased for exploitation by cyber criminals, leading to a rise in cyber threats and incidents. This urgency to adapt to remote operations potentially resulted in oversights in cybersecurity measures, making organizations more vulnerable to attacks, particularly in critical infrastructure sectors (Garcia-Perez, Sallos and Tiwasing, 2023). The global pandemic set thus the stage for a substantial surge in cybercrimes, with a notable increase in cyber-dependent crimes such as hacking, malware, online fraud, phishing, and DDoS

attacks, particularly during the strictest lockdown measures (Buil-Gil et al., 2021). Ethical hacking, also known as white hat hacking, encompasses the practice of using hacking skills for defensive and constructive purposes (Rathore, 2016). Ethical hackers are pivotal in identifying vulnerabilities in networks and systems, thereby allowing organizations to secure their infrastructure from potential cyber threats (David & Smiley, 2022; Rathore, 2016). They play a critical role in providing organizations with opportunities to reveal weaknesses and administer countermeasures before black hat hackers exploit vulnerabilities, thus safeguarding against unauthorized access (David & Smiley, 2022). Overall, its ongoing significance is attributed to its pivotal role in mitigating risks, protecting systems and data, and maintaining security measures in the ever-evolving landscape of cyber threats. However, recent years have witnessed a surge in cyber-attacks and data breaches, highlighting an urgent need for skilled cybersecurity professionals (Tang et al., 2017; Bowen, 2017;). Consequently, cybersecurity degrees have garnered a national priority, yet the field faces a critical shortage of adequately qualified professionals (Gross & Ho, 2021).

The lack of cyber defenders goes beyond a competent technical background since studies have shown a mismatch between education provisions and essential industrial skills, particularly among recent graduates (Chhetri, 2023). Given the urgent demand for qualified cybersecurity professionals and the evident gaps in educational provisions, it is crucial to explore certifications capable of bridging this skills gap. Institutes of higher education (HEI) stress the significance of acquiring such certifications, considering them among the many advantages that can set apart cybersecurity professionals in the marketplace. This includes vendor-neutral certifications such as the Certified Information Systems Security Professional (CISSP), regarded as the golden standard in the field, the Certified Information Systems Auditor (CISA) certificate from ISACA, valuable for IT management roles, and CompTIA Security+, an entry-level certification covering fundamental concepts and practices (Knapp et al., 2017, p.105). The second category encompasses vendor-specific certifications, notably the Cisco Certified Network Associate Security (CCNA Security) which covers essential security skills needed to navigate Cisco network devices, and the Certified Ethical Hacker (CEH), a comprehensive certification in ethical hacking (Knapp et al., 2017, p.105-107). Lastly, attention is drawn to certifications that have recently gained prominence in the market, such as the Cloud Security Professional (CSP) highlighting the importance of cloud security skills, and the Offensive Security Certified Professional (OSCP), focusing on advanced penetration testing skills for professionals (Knapp et al., 2017, p.107-108). The need to develop a novel pedagogical approach in conducting ethical hacking and penetration testing in HEI capable of bridging the skill gap required to build graduates in industry-rooted skills is therefore a growing concern. While each mentioned certificate holds intrinsic value within the market, it is important to note that they do not supplant the significance of a cybersecurity diploma or other relevant certifications in the field.

Whilst it is important to grow beyond the knowledge provided in a typical HEI and the corresponding degrees, the fundamental problem still resides in how educational institutions mostly rely on teaching methods that lean towards theoretical frameworks and compliance, which in return lack emphasis on practical technical skills and soft skills (Bowen, 2017). These limitations have prompted the integration of operation-based exercises and shedding light on hands-on skill development(Sánchez et al., 2020), a phenomenon which has shown promise in addressing the skill gaps within the pedagogy of cyber security (Taylor-Jackson et al., 2020). Existing studies that attempt to develop a hands-on approach to ethical hacking within the HEI pedagogy generally suffer from robustness and student-centered learning (Bhatia et al. 2023; Barman et al. 2023). Given that artificial intelligence has been widely deployed in areas such as intrusion detection and response systems, anomaly, and behavioral profiling, as well as intuitive malware analysis, this study posits that such can be leveraged to provide a robust learning framework. Furthermore, the demand for AI-powered tools capable of alleviating the burden of memorization has surged (Heim et al., 2023). This raises the question: Can AI serve not only as a tool for penetration testing but also to effectively train the penetration testers themselves? This is particularly pertinent for Large Language Models (LLMs). This study therefore proposes a student-centered learning process called PentHack— a tool designed to incorporate a human-AI collaborative approach into the ethical hacking lifecycle. The study by Chhetri (2023) highlights the effectiveness of personalized learning experiences in establishing a solid foundation for beginner penetration testers. Through PentHack, this study aims to harness AI technology, offering personalized learning across various skill levels within the penetration testing lifecycle. This approach aims to streamline the learning curve for HEI students in this field. To the best of the Authors' knowledge, this is the first study to explore the development of a learning platform that integrates LLMs with the learning process of hacking. Furthermore, the study conducted both usability and adoption tests for the developed platform. The remainder of the manuscript is structured as follows: section II provides a brief study on related works targeted at the ethical hacking (and penetration testing) process in HEI. A detailed breakdown of the methodology is

provided in Section III while the result and analysis of the developed tool are provided in Section IV. Discussion and conclusion are provided in Section V and Section VI respectively.

The literature reveals that Large Language Models (LLMs) are playing a transformative role in cybersecurity, enhancing security information and event management (SIEM) systems (Pulyala, 2023). These AI-powered models, integrated with machine learning and natural language processing capabilities, are enabling more efficient threat detection and response mechanisms in the face of evolving cyber threats. In education, LLMs like ChatGPT are being explored for their potential to revolutionize academic practices and pedagogical experiences (Grassini, 2023). Several studies have highlighted the instrumental role of AI technologies in various educational activities, from essay grading to enhancing the learning process through automation and personalized feedback mechanisms. Moreover, the intersection of AI and academic integrity is a subject of increasing scrutiny (Gustilo et al., 2024). With the advent of algorithmically driven writing tools, educators are facing new challenges and ethical considerations in ensuring academic integrity standards while leveraging AI technologies to enhance students' learning experiences and writing proficiency. Overall, these documents underscore the significant potential of AI technologies, including LLMs, in transforming various sectors such as cybersecurity and education. However, alongside the benefits, there is a growing emphasis on addressing ethical implications, ensuring data privacy, and maintaining academic integrity standards in the deployment of these advanced technologies. By encompassing these key insights from the documents, it is evident that AI technologies, particularly LLMs, are reshaping traditional practices and methodologies in diverse spheres, leading to both opportunities and challenges that need to be carefully navigated for the realization of their full potential.

2. Related Works

Numerous pedagogical methods within cybersecurity education have come to light, aiming to optimize student learning experiences by integrating various approaches. Active Learning, exemplified by interactive activities and hands-on exercises, enhances comprehension and retention of cybersecurity concepts by encouraging students to actively connect ideas (Bowen, 2017; Gross & Ho, 2021). Problem-Based Learning (PBL), a student-centered approach, fosters critical thinking and practical application of knowledge through collaborative solving of real-world cybersecurity challenges (Shivapurkar et al., 2020). Psychological Integration integrates behavioral theories into cybersecurity education, improving problem-solving skills and enabling students to discern criminal motivations beyond technical concepts (Shivapurkar et al., 2020). Innovative pedagogical approaches, inspired by web-based learning theory, create immersive training interfaces that engage learners in simulated cyber threat scenarios, promoting theoretical understanding and practical competencies (Tang et al., 2017).. The amalgamation of these methodologies forms a comprehensive pedagogical framework in cybersecurity education, nurturing technical proficiency alongside critical thinking, adaptability, and a profound comprehension of cyber threats and human vulnerabilities. This holistic approach addresses the multifaceted nature of the field, producing well-rounded cybersecurity professionals. This perspective is supported by Bhatia et al. (2023) which asserts that ethical hacking and network security curriculum development should follow a problem-based learning approach. The study suggests mapping the phases of ethical hacking, particularly reconnaissance and enumeration, to the MITRE ATT&CK framework. Whilst the mapping to the MITRE framework can provide a good benchmark process, it failed to ensure a robust learning process for students in HEI. Similarly, the study by Barman et al. (2023) developed a framework for conducting reconnaissance and enumeration using relevant tools and their associated commands. The study further provides a baseline for effectively delivering ethical hacking courses to HEI students. However, the study failed to provide a robust baseline for problem-solving learning. Furthermore, it demonstrated that it is limited to only two stages in the hacking lifecycle.

A study by Yu et al. (2023) considers the integration of LLMs into the penetration testing process, albeit, for Red teamers. The study developed a GPTFUZZER; a tool that can automate the process of generating templates for jailbreaking any LLM towards producing *any* desired output. The study further evaluated the effectiveness of template generation of GPTFUZZER with ChatGPT, LLaMa-2, and Vicuna. Suffice it to say that the study provides a useful insight into LLM jailbreaking which may not be required for an HEI ethical hacking course. Happe and Cito (2023) assert that there are pieces of evidence to suggest that penetration testers have begun experimenting with generative AI to complete the last phase of the ethical hacking lifecycle. Based on this assertion, the study further attempts to answer the question: "*To what extent can we automate security testing with LLMs?*". The study leveraged the knowledge base of the MITRE ATT&CK framework to align the tactics, techniques and procedures used by attackers with the proposed LLM-induced hacking process. By using AgentGPT, AutoGPT, and GPT3.5 the study experimented on two use cases: low- and high-level prompts applicable to penetration

testers. The result presented in the study shows the potential relevance of the study to penetration testers. However, this still lacks the educational construct where HEI students can follow a creative learning curve which can be built on. These studies lend credence to the need for a more robust problem-solving learning mechanism suitable for all students within the learning spectrum. The methodology adopted for the development and evaluation of the proposed PentHack is provided in the next section.

3. Methodology

To develop the proposed PentHack, the operational framework presented in Figure 1 is leveraged. This framework comprises three interconnected phases. In Phase I, exhaustive research was undertaken to ensure that the tool met the foundational expectations of an educational platform. This involved a thorough examination of various aspects, including the university's cybersecurity curriculum, particularly focusing on courses geared towards educating beginner ethical hackers. Additionally, recent pedagogical methodologies supporting interactive teaching methods for students were explored. Through this research phase, the core system requirements and optional system requirements of the tool were finalized, as depicted in Figure 1, utilizing agile methodology. Furthermore, this phase includes the characterization of pedagogical principles within the design of the functional model.

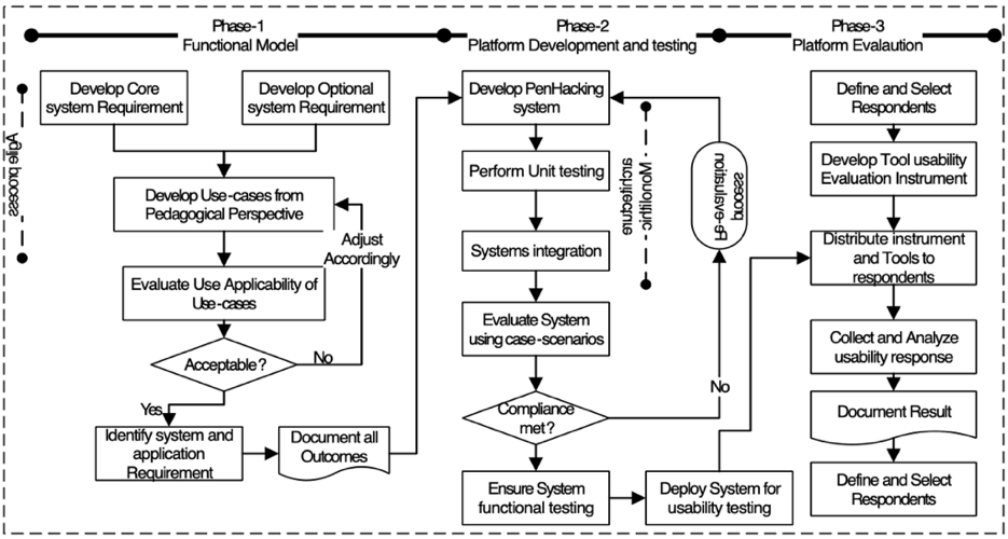

Figure 1: Operational framework of the proposed PentHack Platform

The output of the first phase is parsed as input to the second phase. During the second phase of PentHack's development, a monolithic architecture was implemented to streamline the development and testing processes. The platform was built as a single, cohesive unit, encompassing the graphical user interface (GUI) layer, logical layer, and Thesedata access layer.

To ensure the platform's quality and reliability, extensive unit testing was conducted to validate the functionality of individual components independently. Comprehensive testing measures were implemented to identify and rectify any potential bugs or errors that users might encounter during tool usage. Conducting testing concurrently with development enabled the identification of issues, such as the failure of response from the AI, failure to use and optimize prompt engineering, and several function and class overwriting. These issues were promptly addressed, ensuring the stability and reliability of the platform.

PentHack was developed using Python as the programming language. The application utilized various libraries such as Tkinter, customTkinter, datetime, reportlab.lib, and Pillow. Detailed evaluations were conducted on various AI technologies, including Google BERT, Microsoft's LLM, OpenAI's GPT-3, and GPT-4. API keys were integrated to incorporate LLM functionalities into the application. After extensive evaluation, OpenAI's GPT-4 was integrate into PentHack for its superior security, top-notch performance, and widespread adoption among developers.

In the third phase, a usability and relevance test is carried out. Three constructs in the Technology Adoption Model (Pranoto and Lumbantobing, 2021) were adapted to evaluate the platform. A synopsis of the construct and the measurement items is further provided in Table 1. The 5-point Likert scale was adopted for this study.

Perceived ease of Use (PEU) and Perceived Usefulness (PU) were used as the dependent variables, and Behavioral Intention to Use (BIU), the independent variable. Thus, the following null hypotheses are defined:

1. There is no statistically significant relationship between PEU and BIU ($H_0$1)
2. The relationship between PU and BIU is not statistically significant ($H_0$2).

The logic of leveraging PU is to measure the potential benefit and relevance of the developed tool. PEU on the other hand was adopted to measure the perceived level of ease of using this platform. Both PEU and PU therefore provide a user evaluation of the proposed platform. BIU is a construct which reflects the tendency of the respondents to use the proposed platform for their ethical hacking classes. The platform was put under evaluation by students enrolled in a university ethical hacking course. The students were eligible for the evaluation as they were actively engaged in studying ethical hacking and were therefore well-positioned to provide insights into the importance and effectiveness (or otherwise) of the developed PentHack platform. Following ethical clearance approval, students were recruited to participate in the study voluntarily, without any form of incentive or compensation. A total of 39 students partook in the evaluation process of the platform, with 70:30 female: male distribution. SmartPLS 4.0 was used to analyze the relationship between variables (BIU<--PU and BIU<--PEU).

Table 1: Summary of the Evaluation Instrument.

CONSTRUCT	QUESTIONS
Perceived Ease of Use (PEU)	PEU1: Overall, the tool seems to be easy to use
	PEU2: Learning to operate the application would be easy for me due to its intuitive user interface.
	PEU3: I find the application simple to use due to its user-friendly design and clear content presentation.
Behavioral Intention to Use (BIU)	BIU1: If available, I intend to use this application as it corresponds with my educational goals and needs.
	BIU2: I intend to add this tool to my list of tools for the ethical hacking course as it provides further guidance on the ethical hacking steps and phases.
	BIU3: If available, I intend to use this tool for my ethical hacking course to aid my understanding
Perceived Usefulness (PU)	PU1: This application will be useful and valuable in my ethical hacking journey.
	PU2: The application will be useful for obtaining a fundamental understanding of the ethical hacking phases.
	PU3: The application will be useful in remembering commands and how to use them.
	PU4: I believed that using the application would improve my ability to comprehend ethical hacking principles.

4. Result and Analysis

The study's findings provided vital insight into the PentHack platform's effectiveness in addressing the cybersecurity skills gap. The evaluation approach comprised usability and relevance testing, which were then completed through a questionnaire, providing numerous critical results. First, usability testing revealed that, while participants generally considered the PentHack platform intuitive and user-friendly, there were certain areas for improvement. Some users had trouble navigating specific features and accessing resources. In addition, feedback on the interface design indicated the need for clearer instructions and more streamlined procedures. These findings showed the significance of fine-tuning the user experience to improve overall usability. Table 2 shows the descriptive statistics of participant responses categorized by their satisfaction levels with the knowledge development tool. It illustrates the mean and standard deviation values for various aspects of the tool's usability and usefulness across different levels of satisfaction, ranging from very dissatisfied to very satisfied.

Table 2: Descriptive Statistics of the Response

Satisfaction Level	Mean Overall Ease of Use	Std. Dev. Overall Ease of Use	Mean Learning Ease	Std. Dev. Learning Ease	Mean User-Friendliness	Std. Dev. User-Friendliness	Mean Intention to Use	Std. Dev. Intention to Use	Mean Usefulness	Std. Dev. Usefulness	Mean Understanding	Std. Dev. Understanding
Very Dissatisfied (1)	-	-	-	-	-	-	-	-	-	-	-	-
Dissatisfied (2)	-	-	-	-	-	-	-	-	-	-	-	-
Neutral (3)	2.8	0.632	3.1	1.249	3.2	0.7	3.3	1.048	3.1	0.829	3.1	1.171
Satisfied (4)	3.9	0.316	3.9	0.7	4.0	0.282	4.0	0.0	4.0	0.447	3.8	0.421
Very Satisfied (5)	4.4	0.875	4.5	0.5	4.4	0.875	4.4	0.875	4.6	0.548	4.3	0.9

Second, the significance of the assessment demonstrated the PentHack platform's applicability to educational goals and industry expectations. The findings revealed that the platform effectively addressed key themes and provided valuable information about penetration testing methodologies. However, some participants expressed concerns about the level of coverage for certain topics and suggested additional resources or modules to augment learning. This underscores the need to ensure that the platform effectively addresses the diverse needs of cybersecurity learners.

Overall, while the PentHack platform shows potential as a tool for bridging skill gaps in cybersecurity education, more refinement is required to enhance its effectiveness. The findings of usability and relevance testing gave useful feedback for iterative changes, which will guide future development efforts.

The result of the structural analysis used for testing the hypothesis is presented in Table 3. Using a bootstrap of 5000 samples, the reliability, average variance explained (AVE), and composite reliability (CR) of the measurement model satisfied the standard thumb rule for a measurement model. Furthermore, the loading (outer loading) for all measurement items was greater than the standardized 0.5 regression weight as highlighted in Figure 1.

Table 3: Analysis of the Measurement model

Construct	Cronbach's alpha	AVE	CR
Perceived Ease of Use (PEU)	0.943	0.897	0.947
Behavioral Intention to Use (BIU)	0.930	0.877	0.94
Perceived Usefulness (PU)	0.967	0.910	0.968

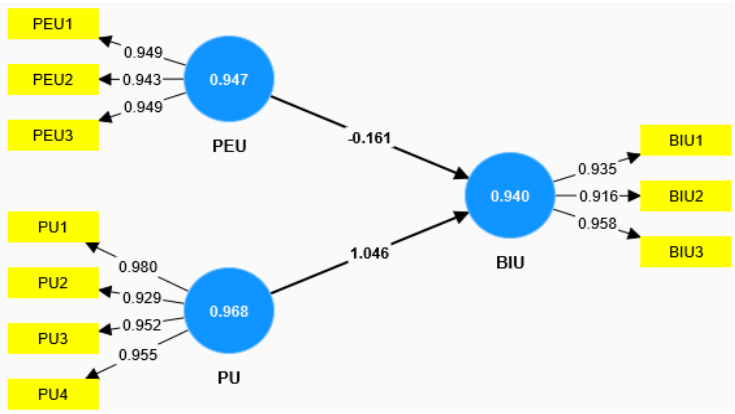

Figure 2: Measurment model of the evaluation process

Given the result of the measurement model, the structural model (further shown in Figure 2) was used to test the stated hypothesis of the study. The relationship between BIU<-- PU generated a statistically significant relationship at *p*-value <0.05. This implies that the null hypothesis, $H_0 2$, can be rejected in favor of the alternate hypothesis. However, the relationship between BIU<--PEU generated a statistically insignificant result with a *p*-value >0.05, as shown in Figure 1. Thus, the null hypothesis, $H_0 1$, is accepted.

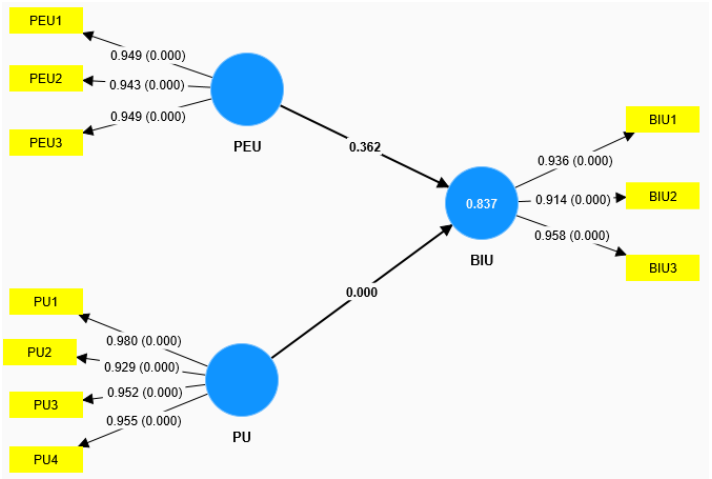

Figure 3: Structural model showing the *P*-value of the relationships.

By accepting the null hypothesis, $H_0 1$, the model result suggests that the respondents opine that the perceived overall presentation and ergonomics of the developed platform would likely not induce their intention to use the platform for their ethical hacking lessons. This position aligns with the overall descriptive analysis. Also, it supports the notion that the developed platform is a preliminary prototype which would be advanced further. Conversely, by rejecting the null hypothesis, $H_0 2$, in favor of the alternate hypothesis, the model suggests that the respondents strongly opine that the developed platform is conceptually relevant and useful for ethical hacking lessons. This perception would in turn induce the tendency to use the platform for ethical hacking classes. Given that the platform is infused with a pedagogical perspective, the result of the model further highlights the agreement of the respondents to the potential of the platform.

5. Discussion

The PentHack platform represents a significant effort to address these gaps by employing AI technology to create personalized learning experiences. However, assessing the platform's usability and relevance reveals room for development, particularly in terms of user-friendliness and alignment with educational aims. Despite these limitations, the research contributes significantly to the industry by suggesting a viable solution to the skills gap mentioned.

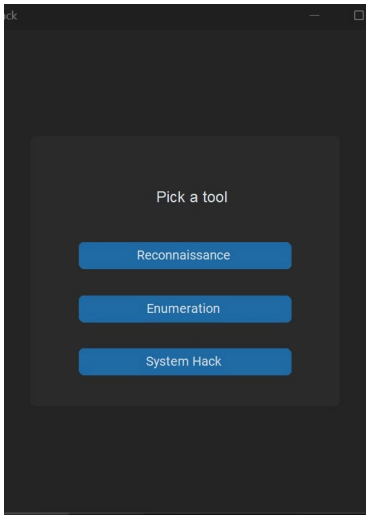

Figure 4.1: First window after user login

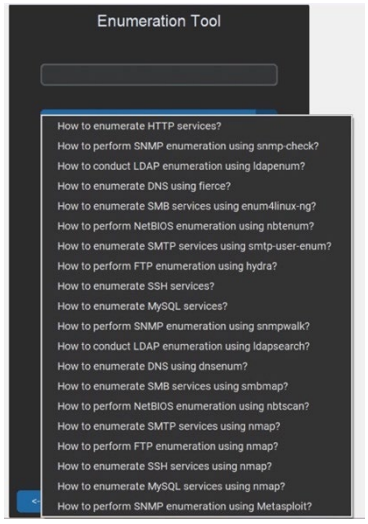

Figure 4.2: built-in prompts for user

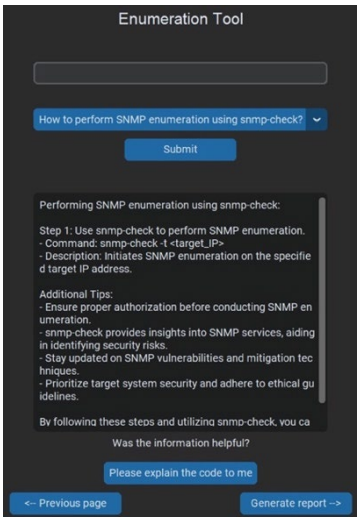

Figure 4.3: displayed built-in responses

Moving forward, more research is needed to increase the PentHack platform's effectiveness and scalability while simultaneously tackling rising cyber threats. The study introduces an academic-focused penetration testing

learning platform, integrating large language models (LLMs) to offer user-friendly ethical hacking tools. Highlighting the pressing need for innovative pedagogical approaches within CS education. Similarly to Chhetri's study on pedagogical approaches in teaching penetration testing to beginner pen-testers, shedding light on the importance of a customized, project-based learning experience (Chhetri, 2023), the study focused on offering a full course in penetration testing for a wider sample of demographics, whereas our goal is to elevate the learning experience of students by offering a more customized approach for students, having each student make use of the platform in their preferred way.

It goes to show how the need for innovative pedagogical approaches in cybersecurity education is crucial to bridging the skills gap and adapting to emerging cyber threats. Moreover, it is crucial to acknowledge the limitations encountered during the evaluation process, the survey conducted to assess the PentHack platform's effectiveness in bridging the cybersecurity skills gap provided valuable insights, explicitly regarding its usability and alignment with educational goals. Overall, respondents expressed positive experiences with the platform's usability with the identified areas for improvement. Despite the insightful feedback received from survey respondents regarding PentHack usability and relevance, the findings were interpreted with caution due to the sample size limitation. With the limited number of participants, the scope of the survey findings may be constrained, as the insights gathered represent a specific subset of the population. The small sample size limits the ability to extend the findings to a broader audience or make definitive claims about the platform's overall effectiveness in addressing cybersecurity skills gaps. Moving forward, it is recommended to consider expanding the sample size in future surveys or usability testing to capture a broader range of perspectives and experiences, as it can be more representative and offer deeper insights into the platform's efficacy in educational settings. Additionally, leveraging a larger sample size can enhance the statistical validity of the survey results and support more conclusive recommendations for refining the PentHack platform and other AI-integrated tools in cybersecurity education.

6. Conclusion

This paper introduced and detailed the evolution and significance of the internet, emphasizing its revolutionary role in society and current technological advancements. The presented work created a variety of significant insights into the chosen topic in cyber security learning, as well as the development of unique pedagogical approaches. Furthermore, it correctly contextualizes the necessity of cybersecurity in today's digital landscape, particularly in light of COVID-19's impact on digital reliance. Furthermore, the examination of relevant works provides a comprehensive overview of existing material, indicating gaps in current instructional approaches and possibilities for improvement. To summarize, the outcome of this study highlights the necessity of new pedagogical techniques in meeting the changing needs of education in cybersecurity. The PentHack platform could therefore be a significant advancement in offering students immersive, hands-on learning experiences in the field of ethical hacking. With that, the platform has the potential to revolutionize cybersecurity education by leveraging AI technology and individualized learning approaches, empowering students to address increasingly complex problems. As an ongoing work, the proposed platform will be further enhanced with several user-input processes. In addition, the platform will integrate immersive learning experiences through virtual and augmented reality which could help develop an action-consequence paradigm in users.

References

Bhatia, S., Elhadad, S., Deshmukh, A., Yellela, M.K. and Vangala, O.S.R., 2022, March. Hack The Problem: A Problem-Based Learning Approach for Ethical Hacking and Network Defense Curriculum. In Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 2 (pp. 1346-1346).

Barman, F., Alkaabi, N., Almenhali, H., Alshedi, M., & Ikuesan, R. (2023). A Methodical Framework for Conducting Reconnaissance and Enumeration in the Ethical Hacking Lifecycle. Retrieved from https://papers.academic-conferences.org/index.php/eccws/article/download/1438/1148

Bowen, L. M. (2017). The Limits of Hacking Composition Pedagogy. Computers and Composition, 43, 1-14.

Buil-Gil, D., et al. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. European Societies, 23(sup1), S47–S59. https://doi.org/10.1080/14616696.2020.1804973

Castells, M. (2019). The Impact of the Internet on Society: A Global Perspective. OpenMind. Retrieved from https://www.bbvaopenmind.com/en/articles/the-impact-of-the-internet-on-society-a-global-perspective/

Chhetri, C. (2023). "It was a one of a kind experience:" Student Experiences and Pedagogical Design of a Project-based Hands-on Cybersecurity Pen-testing Course. In Proceedings of the 24th Annual Conference on Information Technology Education (pp. 22-27).

David, E., & Smiley, G. (2022). An Ethical Framework for Cybersecurity Professionals: A Grounded Theory Study. ProQuest Dissertations and Theses. Retrieved from https://www.proquest.com/dissertations-theses/ethical-framework-cybersecurity-professionals/docview/2746081552/se-2?accountid=15192

De Paoli, S., & Johnstone, J. (2023). A qualitative study of penetration testers and what they can tell us about information security in organisations. Information Technology & People [Preprint]. https://doi.org/10.1108/ITP-11-2021-0864

Duan, Y., Edwards, J. S., & Dwivedi, Y. K. (2019). Artificial Intelligence for Decision Making in the Era of Big Data – evolution, Challenges and Research Agenda. International Journal of Information Management, 48, 63–71.

Garcia-Perez, A., Sallos, M. P., & Tiwasing, P. (2023). Dimensions of cybersecurity performance and crisis response in critical infrastructure organizations: an intellectual capital perspective. Journal of Intellectual Capital, 24(2), 465–486. https://doi.org/10.1108/JIC-06-2021-0166

Graham, M., & Dutton, W. H. (2019). Society and the Internet: How Networks of Information and Communication are Changing Our Lives. Oxford University Press. Retrieved from https://books.google.ae/books?hl=en&lr=&id=vdShDwAAQBAJ&oi=fnd&pg=PP1&dq=social+and+cultural+impacts+of+the+Internet&ots=zIAUf9Omi0&sig=WOGxG_z8FTcsmpvOZI4BlaewHvg&redir_esc=y#v=onepage&q&f=false

Grassini, S. (2023). Shaping the Future of Education: Exploring the Potential and Consequences of AI and ChatGPT in Educational Settings. In Education Sciences (Vol. 13, Issue 7). Multidisciplinary Digital Publishing Institute (MDPI). https://doi.org/10.3390/educsci13070692

Gross, M., & Ho, S. M. (2021). Collective learning for developing cyber defense consciousness: an activity system analysis. Journal of Information Systems Education, 32(1), 65-76.

Gustilo, L., Ong, E., & Lapinid, M. R. (2024). Algorithmically-driven writing and academic integrity: exploring educators' practices, perceptions, and policies in AI era. International Journal for Educational Integrity, 20(1), 3. https://doi.org/10.1007/s40979-024-00153-8

Happe, A. and Cito, J., 2023, November. Understanding Hackers' Work: An Empirical Study of Offensive Security Practitioners. In Proceedings of the 31st ACM Joint European Software Engineering Conference and Symposium on the Foundations of Software Engineering (pp. 1669-1680).

Heim, M.P., Starckjohann, N. and Torgersen, M., 2023. The Convergence of AI and Cybersecurity: An Examination of ChatGPT's Role in Penetration Testing and its Ethical and Legal Implications (Bachelor's thesis, NTNU).

Kaur, R., Gabrijelčič, D., & Klobučar, T. (2023). Artificial intelligence for cybersecurity: Literature review and future research directions. Information Fusion, 97, 101804. https://doi.org/10.1016/J.INFFUS.2023.101804

Knapp, K. J., Maurer, C., & Plachkinova, M. (2017). Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. Journal of Information Systems Education, 28(2), 101.

Koutsikouri, D., Lindgren, R., Henfridsson, O., & Rudmark, D. (2018). Extending Digital Infrastructures: A Typology of Growth Tactics. Journal of the Association for Information Systems.

Navarria, G. (2016). How the Internet was born: from the ARPANET to the Internet.

Pranoto, A. H. and Lumbantobing, P. (2021) 'The Acceptance Technology Model for Adoption of Social Media Marketing in Jabodetabek', *The Winners*, 22(1), pp. 75–88.

Pulyala, S.R. 2023, "The Future of SIEM in a Machine Learning-Driven Cybersecurity Landscape", Turkish Journal of Computer and Mathematics Education, vol. 14, no. 3, pp. 1309-1314.

Sánchez, J., Mallorquí, A., Briones, A., Zaballos, A. and Corral, G. (2020). An integral pedagogical strategy for teaching and learning IoT cybersecurity. Sensors, 20(14), p.3970.

Shivapurkar, M., Bhatia, S. and Ahmed, I., 2020, July. Problem-based learning for cybersecurity education. In Journal of The Colloquium for Information Systems Security Education (Vol. 7, No. 1, pp. 6-6).

Tang, D., Pham, C., Chinen, K.I. and Beuran, R. (2017). Interactive cybersecurity defense training inspired by web-based learning theory. In 2017 IEEE 9th International Conference on Engineering Education (ICEED) (pp. 90-95). IEEE.

Taylor-Jackson, J., McAlaney, J., Foster, J.L., Bello, A., Maurushat, A. and Dale, J. (2020). Incorporating psychology into cyber security education: a pedagogical approach. In Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24 (pp. 207-217). Springer International Publishing.

Yu, J., Lin, X. and Xing, X., 2023. Gptfuzzer: Red teaming large language models with auto-generated jailbreak prompts. *arXiv preprint arXiv:2309.10253*.§