Revista Iberoamericana para la Investigación y el Desarrollo Educativo
ISSN 2007 - 7467

https://doi.org/10.23913/ride.v15i29.2052

Scientific articles

EthkLab: laboratorio de bajo costo para aprendizaje práctico en temas de ciberseguridad

EthkLab: Low-cost laboratory for hands-on learning in cybersecurity issues

EthkLab: laboratório de baixo custo para aprendizagem prática em temas de segurança cibernética

Holzen Atocha Martínez-García
Tecnológico Nacional de México / Instituto Tecnológico Superior Progreso, México
holzen.mg@progreso.tecnm.mx
https://orcid.org/0000-0003-0591-0049

Enrique Camacho-Pérez
Universidad Autónoma de Yucatán, México
enrique.camacho@correo.uady.mx
https://orcid.org/0000-0002-2581-1921

Ligia Beatriz Chuc-Us
Tecnológico Nacional de México / Instituto Tecnológico Superior Progreso, México
ligia.cu@progreso.tecnm.mx
https://orcid.org/0000-0002-6433-630X

Resumen

En este artículo se presenta EthkLab, un laboratorio portátil y de bajo costo para el aprendizaje en ciberseguridad y *hacking* ético. El objetivo fue desarrollar un entorno de aprendizaje para estudiantes del Tecnológico Nacional de México campus Progreso, los cuales carecen de un laboratorio especializado en ciberseguridad. Para eso, en primer lugar, se evalúa la viabilidad de la construcción de dicho laboratorio y, posteriormente, se diseña la arquitectura específica de *hardware* y se desarrolla el prototipo. Para validar el laboratorio se efectuaron diversas pruebas con estudiantes voluntarios, las cuales arrojaron resultados satisfactorios que respaldan la hipótesis de que puede ser empleado en beneficio de los estudiantes y potenciar el desarrollo de sus habilidades mediante pruebas prácticas realistas. Sin embargo, como en todo desarrollo preliminar, se identificaron áreas de oportunidad que

deberán ser evaluadas y mejoradas en futuros trabajos sobre esta arquitectura propuesta, la cual es escalable tanto vertical como horizontalmente debido a la naturaleza de su diseño.

Palabras clave: aprendizaje práctico, ciberseguridad, entorno de aprendizaje, laboratorio portátil.

Abstract

EthkLab, a low-cost portable laboratory for learning cybersecurity and ethical hacking, is presented. The objective was to develop a learning environment for students at the Tecnológico Nacional de México campus Progreso, who lack a specialized laboratory about cybersecurity. First, it is defined whether it is possible and feasible to build such a laboratory. Then the specific hardware architecture is designed, and the prototype is developed. Several tests are applied to volunteer students to validate the lab, revealing satisfactory results that support the hypothesis that it can be used to benefit students and improve their skills with realistic hands-on testing.

As in any preliminary development, areas of opportunity were found to be evaluated and corrected in future work on this proposed architecture, which is vertically and horizontally scalable due to the nature of its design.

Keywords: Learning environment, Cybersecurity, Hands-on learning, Portable lab.

Resumo

Este artigo apresenta o EthkLab, um laboratório portátil e de baixo custo para aprendizagem em segurança cibernética e hacking ético. O objetivo foi desenvolver um ambiente de aprendizagem para alunos do Tecnológico Nacional de México campus Progreso, que carecem de um laboratório especializado em segurança cibernética. Para isso, primeiro avalia-se a viabilidade de construção do referido laboratório e, posteriormente, projeta-se a arquitetura de hardware específica e desenvolve-se o protótipo. Para validar o laboratório, foram realizados diversos testes com alunos voluntários, que produziram resultados satisfatórios que sustentam a hipótese de que o mesmo pode ser utilizado em benefício dos alunos e potenciar o desenvolvimento das suas competências através de testes práticos realistas. No entanto, como em todo o desenvolvimento preliminar, foram identificadas áreas de oportunidade que devem ser avaliadas e melhoradas em trabalhos futuros nesta

arquitectura proposta, que é escalável tanto vertical como horizontalmente devido à natureza do seu design.

Palavras-chave: aprendizagem prática, segurança cibernética, ambiente de aprendizagem, laboratório portátil.

Reception Date: February 2024 **Acceptance Date:** August 2024

Introduction

The persistent shortage of trained personnel in the field of cybersecurity, as evidenced by the 1.8 million vacancies globally in 2021 and the 35,000 unfilled positions in Mexico in areas such as ethical *hacking* and forensic computing, has become a critical challenge (Salazar-Mata *et al.* , 2021). This situation is aggravated by the continuous increase of electronic devices and digital services, which give cybercriminals a wider field of action (Torres-Knight and Méndez-Morales, 2023). The alarming reality is reflected in the 187 billion cyberattack attempts recorded in Mexico during 2022, which represents an increase of 20% compared to the previous year, according to FortiGuard Labs (Fuentes-Penna *et al*., 2023).

Given this scenario, the proposed strategy of creating educational centers specialized in cybersecurity, suggested by Arreola-García (2019), is of great interest, since its teaching from the academy would not only address the urgent need for qualified personnel, but would also be an essential pillar to strengthen the capacity of companies and governments, enabling them to perform their functions in cyberspace in a secure, innovative and effective manner.

Although the massive expansion of specialized cybersecurity educational centers is a challenge, there is growing interest in addressing current problems. Universities and higher education institutes already offer specialized programs, from undergraduate to postgraduate, in areas such as ethical *hacking* and risk management. This comprehensive approach not only seeks to meet the demand for cybersecurity experts, but also to train leaders capable of facing constantly evolving digital challenges. Additionally, some institutions train their staff through practical laboratories.

One of the best ways to learn about cybersecurity is through ethical *hacking laboratories (Pearson et al.*, 2020), that is, it is a space where a real but controlled environment is simulated to allow students to learn how hackers work. security systems, how

to detect vulnerabilities and the techniques to exploit them, so that they comprehensively understand how to adequately protect themselves against these types of attacks.

However, although it is essential that higher education institutions provide the appropriate technological infrastructure to support the comprehensive development of the university student (Muñoz-Martínez, 2020), the reality is usually different, especially in public university education, where there has been no achieved the desired competitiveness compared to other countries. Although public university education is mandatory according to Article 3 of the Mexican Constitution, in practice, institutions do not have adequate infrastructure. This is largely due to the economic context of the country, so that the decree can be considered effective in terms of coverage, but not in terms of improvement. (Velasco-Arellanes *et al.*, 2020).

In the specific case of the Tecnológico Nacional de México campus Progreso, a deficiency is observed in the Computer Systems Engineering career due to the updating of the specialty of the educational program, which in its latest version focuses on cybersecurity, but does not include with a laboratory specialized in that discipline to support student performance.

Therefore, this work focuses on the design and development of a functional prototype of a cybersecurity laboratory that is characterized by being low cost, having realistic environments and contributing to the comprehensive development of students in terms of practical skills in *pentesting* and ethical *hacking.* The proposal offered constitutes a preliminary study to determine the viability of using low-cost technology in the development of a *hardware architecture* that functions as an ethical *hacking laboratory*, with the objective of minimizing costs and spaces for the implementation of a physical training environment. in cybersecurity. The second aspect to evaluate is the adaptability and relevance of the students of Tecnológico Nacional de México to use this architecture.

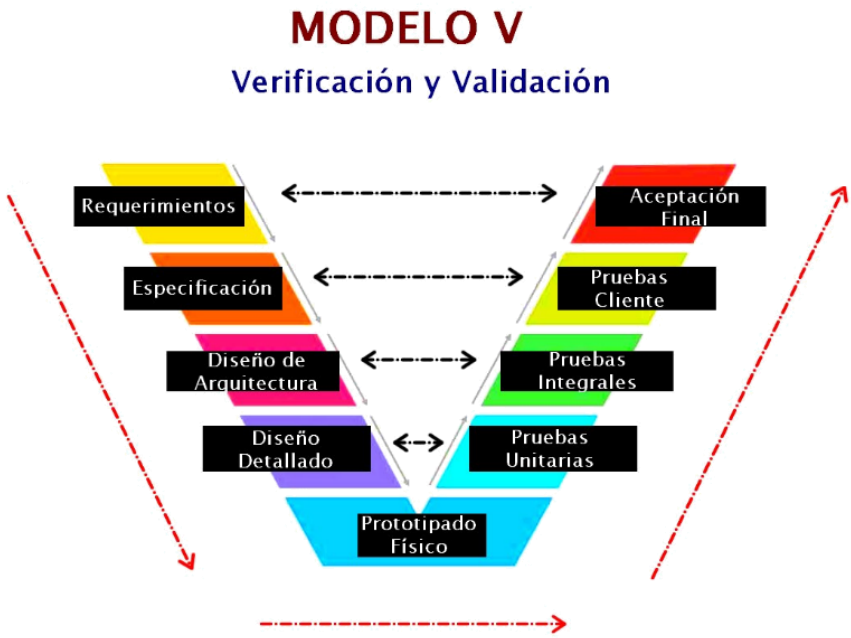
Materials and methods

To determine the feasibility of creating a cybersecurity and ethical *hacking laboratory* with low-cost technology, as a first step a review of the state of the art and technique was carried out with the objective of identifying similar documented prototypes and evaluating their success in implementation or evidence. The search was carried out in the Google Scholar database, using terms such as “cyber range low cost”, “low-cost laboratory”,

"cybersecurity lab ARM" and "SoC lab". From the results obtained, 36 relevant articles were selected based on their title and abstract, and after a complete reading, seven were chosen that presented functional prototypes with ARM architecture devices. Among these, the works of Oh *et al. stood out.* (2020) and by Legg *et al.* (2023), who agreed on the use of Raspberry Pi, a development board with pocket personal computer features.

Then, in the second phase, the architecture of the proposed laboratory was developed, using a validation and verification methodology (Figure 1).

Figure 1. Model used for the development of the laboratory architecture



Source: Own elaboration

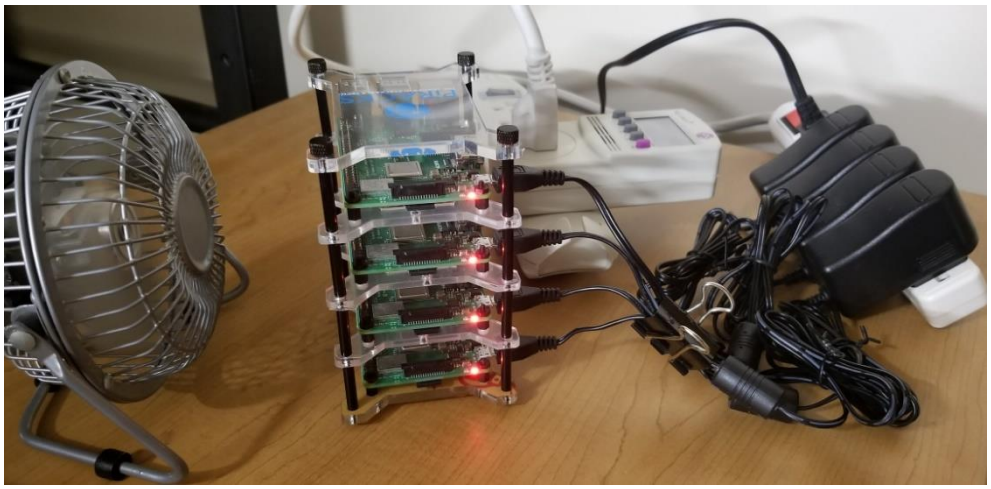
In the validation phase, vulnerable scenarios were configured and tested by a group of 12 volunteer students from the seventh semester of the Institute's Computer Systems Engineering degree. To this end, a survey was designed to evaluate the students' perception of the use and performance of the laboratory. This group was selected because its members are beginning to take courses specializing in cybersecurity.

First phase

As mentioned, seven publications were selected with experimental prototypes that indicated the possibility of generating cybersecurity laboratories for university teaching. Among them, the studies titled *Teaching Web-Attacks on a Raspberry Pi Cyber Range* (Oh *et al*., 2020) and *Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range* (Legg *et al.*, 2023) stood out.

In the proposal by Oh *et al*. (2020) a cybersecurity laboratory focused on web attacks is implemented, deploying a vulnerable web server based on Docker technology and four Raspberry Pi nodes (Figure 2). The analysis concludes that the cost was less than 250 dollars and the energy consumption was less than 25 watts (table 1). Among the conclusions, it is suggested that laboratories built with Raspberry Pi clusters can reduce costs and improve cybersecurity education.

Figure 2. Laboratory cluster with Raspberry Pi 3b+



Source: Oh *et al.* (2020)

Table 1. Raspberry Pi Cyber Range Lab Cluster Power Consumption and Expense Breakdown

Description	Amount	Unit cost in dollars (US)	Total in dollars (US)	Maximum Unit Consumption (Watts)
Raspberry Pi Model 3B+	4	35.00	140.00	4.9
8 GB microSD cards	4	4.99	19.96	
PiRacks Cluster Acrylic Case	1	29.95	29.95	
power source	4	8.99	32.94	
Fan	1	10.99	10.99	5
Grand Total			233.84	24.6

Source: Own elaboration based on Oh *et al.* (2020)

Although the Raspberry Pi Cyber Range may appear visually inelegant, the authors highlight that it efficiently fulfills its original purpose. One of the notable characteristics of this project is its low energy consumption and the cost of the *hardware,* which is below that of a common computer equipment, although it offers sufficient features to run the practice environments.

Regarding the work proposed by Legg *et al.* (2023), a variation in the methodology is offered, since it does not use a cluster as the target server. Instead, the devices are used as independent terminals that interact with a common goal. For this, a Raspberry Pi model with different characteristics is used, the Raspberry Pi 400, which already includes the keyboard as part of the device and has the circuit embedded within it (Figure 3).

A portable monitor and a mouse are added to the Raspberry Pi 400 to function as an independent terminal, and a Raspberry Pi 4 is included as an access point. The prototype with four terminals and an access point, called “UWE Cyber Pi Lab portable setup” by the authors, is shown in Figure 4. This proposal highlights an additional characteristic of laboratories developed with low-cost devices: portability.

Figure 3. Raspberry Pi 400 inside and out

Source: Raspberry Pi Ltd (sf)

Figure 4. UWE Cyber Pi Lab portable setup

Source: Legg *et al.* (2023)

Second phase

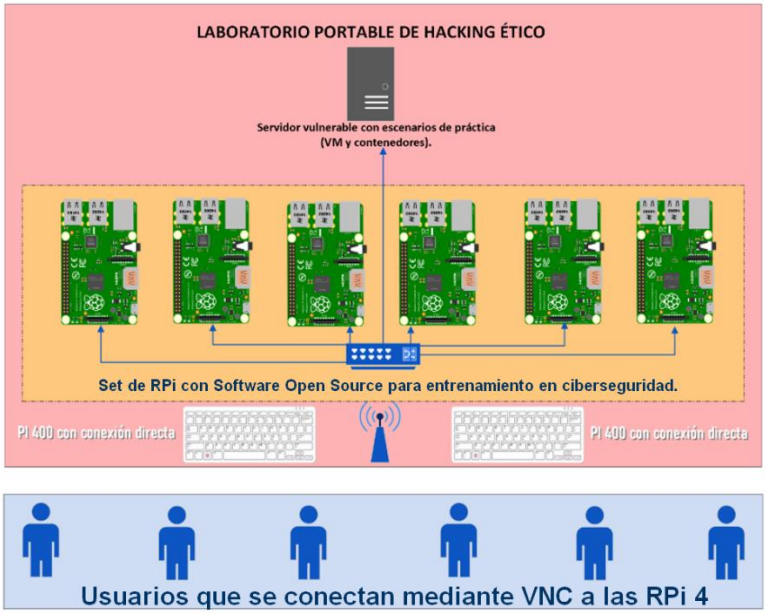
Based on the studies and results examined, it is feasible to answer initial questions about the possibility of establishing an ethical *hacking laboratory* for cybersecurity instruction through the use of low-cost technologies. The affirmative answer is based on several reviewed studies that suggest the use of affordable technologies with sufficient capabilities for the creation of cybersecurity and ethical *hacking laboratories.* Furthermore, it was observed that it is feasible to take advantage of the dimensions of the architecture to achieve an easily transportable laboratory.

Therefore, it was considered plausible to move forward with the project to implement an ethical *hacking* and cybersecurity laboratory for Tecnológico Nacional de México campus Progreso, based on previous studies and local need. Consequently, it was decided to use a

low-cost device called Raspberry Pi, which is portable, approximately the size of a credit card and a few centimeters high. It includes components such as a microprocessor, memory, network card, Wi-Fi card, Bluetooth, sound input, USB ports, HDMI port and power input. In addition, it has GPIO pins that can interact with other electrical or electronic circuits and can be programmed using the Python language through its operating system, making it a versatile and multifunctional device (Martínez-Luengo, 2021).

A first design considered the interconnection of a vulnerable virtual machine server with Raspberry Pi 4 devices as terminals, which contain the necessary *software* to attack vulnerable practice scenarios. To access the terminals, which lack screens, a computer must be connected to the laboratory's internal network and a Raspberry Pi 4 must be remotely controlled using VNC (Virtual Network Computing). VNC uses its own protocol called RFB (Remote Framebuffer Protocol), which allows the transmission of graphic information between the VNC server (on the machine being controlled) and the VNC client (on the machine that performs remote control). Although the option of direct connection to the network with Raspberry Pi 400 equipment was considered, it was later discarded. Figure 5 shows a basic schematic of the original idea.

Figure 5. Preliminary design of the architecture of the proposed laboratory



Source: Own elaboration

After making some changes to the architecture according to the specified requirements, the final list of elements used was as follows (the most relevant are listed):

Table 2. List of elements used for the development of the architecture

AMOUNT	DESCRIPTION	FUNCTION
8	Raspberry Pi 4 B 8GB Ram ARM cortex 1.5 Ghz	*software* installation and configuration to scan and breach test scenarios.
1	MiniPC Intel NUC 10 performance NUC10i7FNKN intel core i7 12 GB Ram 1TB NVMe SSD	Server/target computer that contains the vulnerable scenarios in virtual machines.
1	Monitor Qian QM2151F 21.5" HDMI port	Screen for monitoring the scenario server.
1	TP-Link Dual Band AX Archer AX10 WIFI6 Router	Main router architecture
2	Linksys SE3008 Switch 8 ports 10/100/1000	Interconnection between the RPi and the scenario server.
1	Hadulcet Mobile Computer Station with Wheels, Black.	Part of the mobile laboratory structure.
1	Enson Professional 6U Network Server Wall Cabinet	Container for electrical and wired network connection.
1	Logitech wireless keyboard/mouse kit	Accessories to manipulate the scenario server.

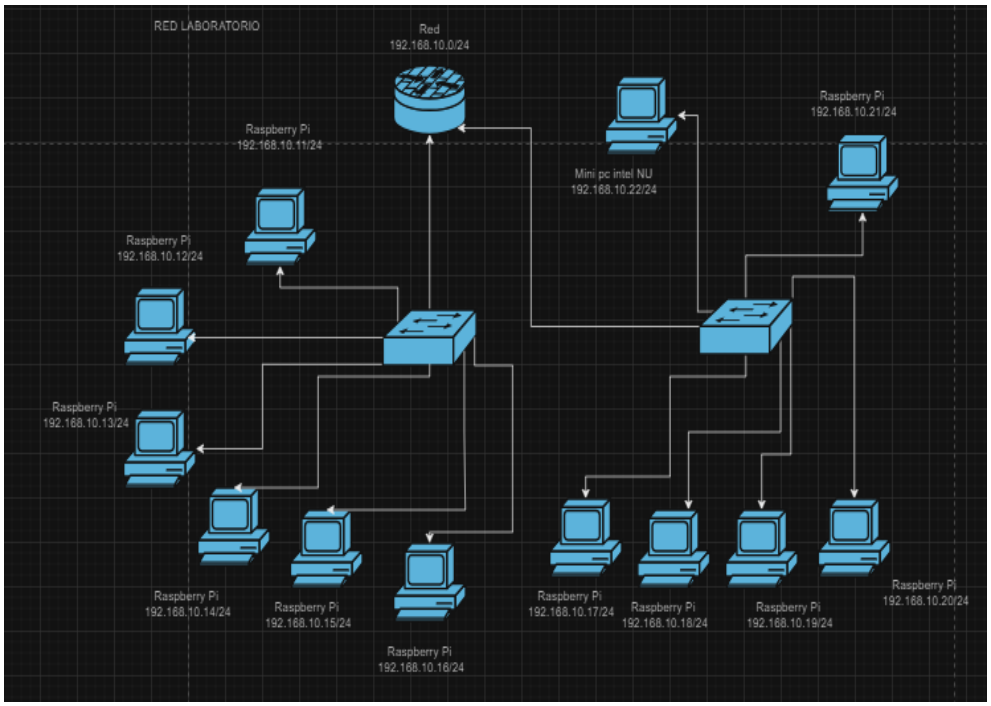
Source: Own elaboration

It is important to emphasize that other accessories were also obtained for the correct operation and maintenance of the proposal, such as electrical wiring, network wiring, periodic backup disk, SD memory cards, among other materials.

Results

Among the results obtained in the analysis of the desired *hardware architecture,* the network scheme described in Figure 6 was developed. The network was designed using a star topology with two *switches* and a *router.* Two methods of IP address assignment were implemented: static IP addresses were assigned to the RPi 4 terminal devices and the scenario server, while dynamic service was enabled for clients connected via wireless network using DHCP (Dynamic Host Configuration Protocol).

Figure 6. Logical network design in the laboratory



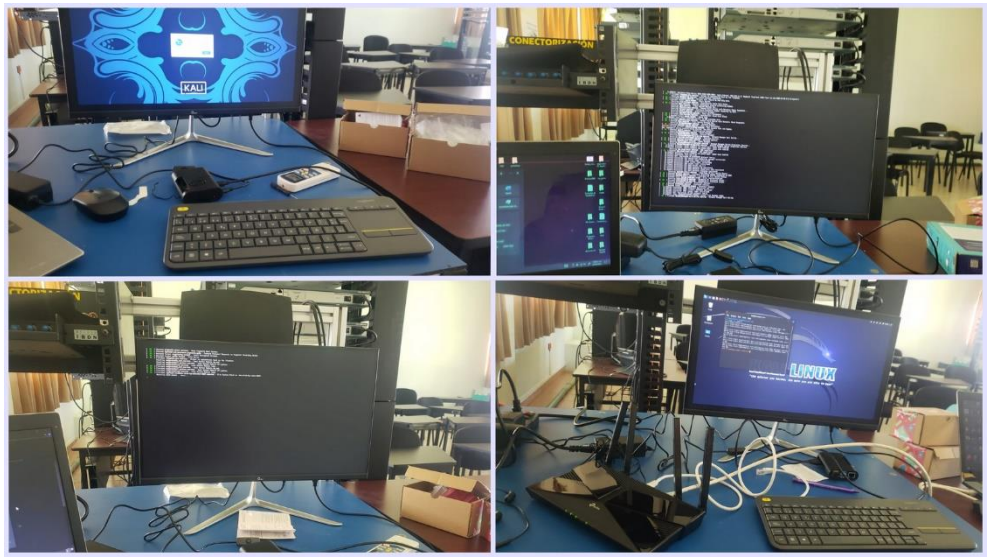
Source: Own elaboration

Next, the physical prototyping of the network was obtained (Figure 7) and the unit tests were started (Figure 8) to verify the proper functioning of each of the devices involved, performing tests individually. In the case of the terminals, the tests focused on power-on and successful network communication. The intermediate devices (*switch* and *router*) were evaluated simultaneously, taking as success parameters the communication between the laboratory devices and the equipment that is connected remotely. Table 3 presents the results obtained in this stage.

Figure 7. Physical prototype of the network architecture

Source: Own elaboration

Figure 8. Unit testing on devices



Source: Own elaboration

Table 3. Unit Test Results

Device	Successful tests	Failed tests	Comments
Raspberry Pi 1 (192.168.0.11)	6	0	No incidents
Raspberry Pi 2 (192.168.0.12)	4	2	In the third and fourth tests it froze at times on the system desktop, not allowing it to work fluidly. A corrupt SD memory problem was noticed, proceeding with the replacement.
Raspberry Pi 3 (192.168.0.13)	6	0	No incidents
Raspberry Pi 4 (192.168.0.14)	6	0	No incidents
Raspberry Pi 5 (192.168.0.15)	6	0	No incidents
Raspberry Pi 6 (192.168.0.16)	6	0	No incidents
Raspberry Pi 7 (192.168.0.17)	6	0	No incidents
Raspberry Pi 8 (192.168.0.18)	6	0	No incidents
LinkSys 1 Switch	24	0	It allowed connectivity and communication with half of the devices during the six tests carried out.
LinkSys 2 Switch	24	0	It allowed connectivity and communication with half of the devices during the six tests carried out.

TP-Link router	45	3	In tests three, eight and 12, incidents were found for assigning the IP address through DHCP to the client laptop. Changes were made to the service configurations until optimal performance was achieved.

Source: Own elaboration

To carry out the comprehensive and client tests, the integration of the elements was completed in the proposed laboratory, as can be seen in Figure 9. Subsequently, the seventh semester group of Computer Systems Engineering at the Tecnológico Nacional de México campus Progreso, was convened to carry out practices in the laboratory (Figure 10).

Figure 9. EthkLab: already integrated laboratory (right and front perspective views)

Source: Own elaboration

Figure 10. Students connected to the laboratory through VNC carrying out ethical *hacking practices*

Source: Own elaboration

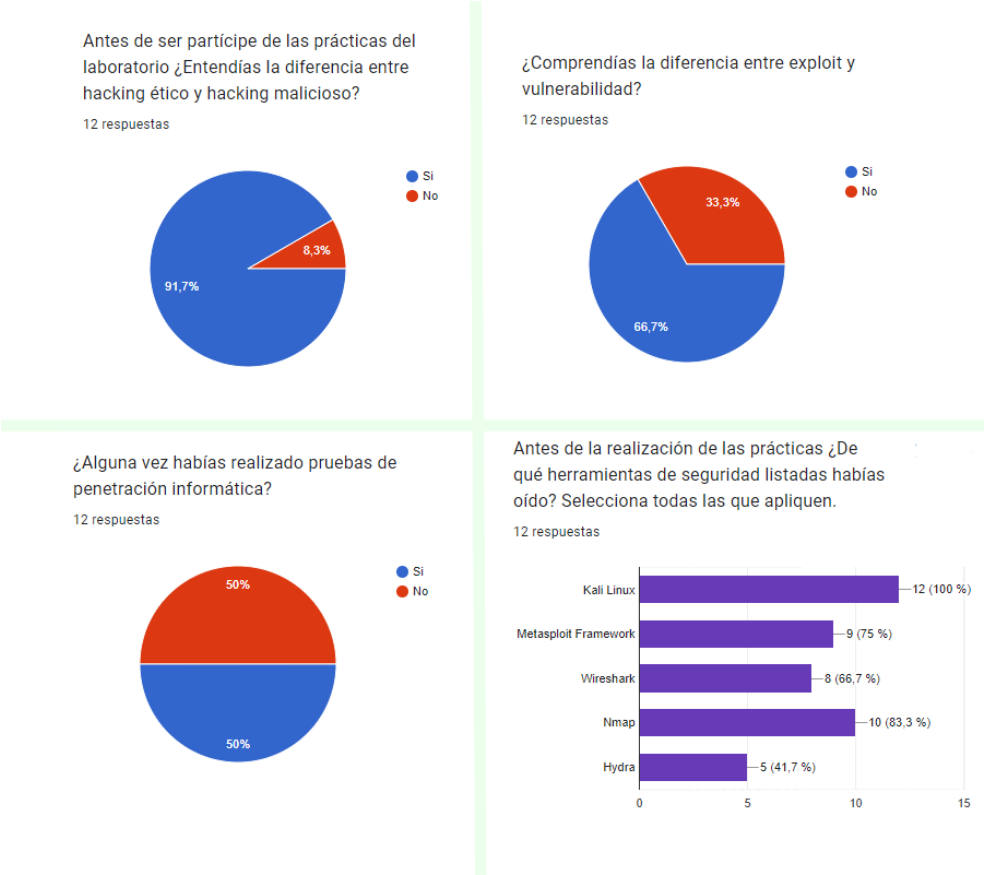
Table 4. Practices carried out by students

Practice number	Qualification	Aim
1	Network scanning	Identify devices on a network and their active services.
2	Vulnerability analysis	Identify possible vulnerabilities in the detected services and systems.
3	Exploitation of known vulnerabilities	Gain unauthorized access to systems to understand the implications of vulnerabilities.
4	Web (In)security	Perform a penetration test on a web server, using a site hosted on it as a gateway.
5	Pentesting (unguided)	Perform a penetration test integrating the concepts and techniques previously studied.

Source: Own elaboration

At the end of the practices, an instrument was applied to the volunteer students. This instrument focused on three main aspects: a) the user's prior knowledge about cybersecurity, b) the user's performance in the EthkLab practices and their own perception after the tests, and c) the user's perception of EthkLab. The most relevant results are presented below.

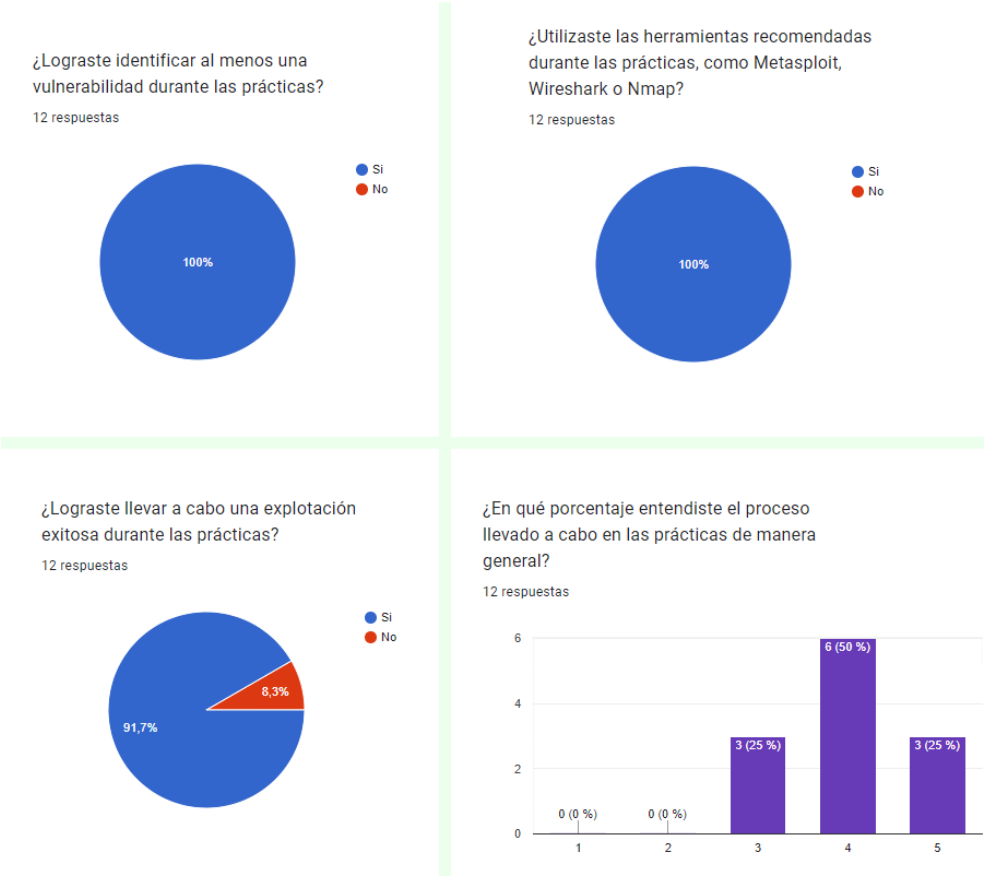
Figure 11. Previous knowledge of users regarding the subject and tools



Source: Own elaboration

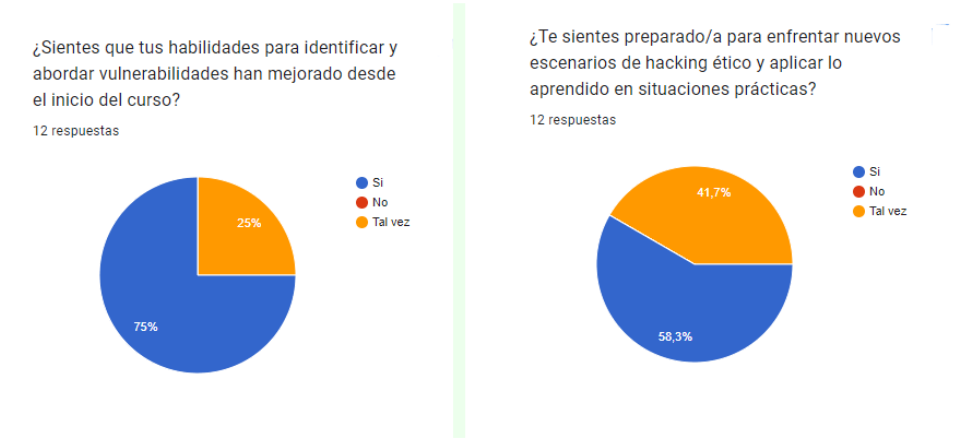
Figure 11 represents the data collected in the first section of the instrument, where the results generally indicate a solid base of cybersecurity knowledge among participants, although with some variations in familiarity with specific tools. For example, most participants report understanding the basics of cybersecurity, and half report having experience in computer penetration testing, suggesting an interest or prior exposure to the field of cybersecurity. In terms of tools, Kali Linux is widely recognized, as well as Metasploit Framework, Wireshark and Nmap; however, Hydra appears to be less familiar to some participants.

Figure 12. Experience of the participants during the practices



Source: Own elaboration

Figure 13. Personal perception after the internship with EthkLab



Source: Own elaboration

Figure 12 shows the data from the second section of the instrument, where all participants stated that they had identified at least one vulnerability during the practices,

indicating effective execution of the activities and the practical application of knowledge in real situations. Additionally, all used the recommended tools, suggesting active application of key tools in penetration testing and vulnerability scanning.

Likewise, the majority achieved successful exploitation, which highlights the effectiveness of their skills in the application of exploitation techniques. Regarding understanding of the process, the majority placed themselves at a reasonable level of four and five on the subjective scale, although some indicated a slightly lower level with a score of three. This aspect can point out areas of improvement or revision for future training sessions that can be adjusted to the objectives and expectations of the course.

Overall, the results indicate good performance, but also offer opportunities for refinement and continuous improvement. This statement is supported by the data shown in Figure 13, where the answers to the last two questions, which focus on personal perception and preparation to face new ethical *hacking scenarios*, reflect a variety of responses. In other words, some participants feel confident, while others express doubt, indicating that improvement in skills does not always translate into complete confidence in applying that knowledge in new situations.

The above may suggest the need for additional pedagogical approaches, continued practice, or resources that reinforce participants' confidence in the practical application of their ethical *hacking skills*. That is, these results provide a comprehensive view of the course experience and potential areas for adjustments or improvements in future iterations of the training program.

Finally, Figure 14 shows that the participants' perception towards EthkLab is mostly positive, as the majority consider that the interface is easy to use and that the integrated tools provided a complete ethical *hacking experience*. In fact, the overall user experience rating is predominantly high, with several responses in the range of four and five. However, some lower scores indicate that some participants may have faced challenges or areas for improvement in the integration of their teams or the effectiveness of certain tools.

Figure 14. Participants' perception of EthkLab

Source: Own elaboration

Discussion

As mentioned by Yamin *et al.* (2020), the first line of defense against cyber threats and crimes is to be aware and prepared, for example, through cybersecurity training, for which dedicated testing platforms and infrastructure are required that facilitate the materialization and execution of scenarios. of training.

In this sense, practical laboratories, also known as *hands-on*, offer valuable experiences that include novel, timely and relevant case studies for the real work environment (Pearson *et al*., 2020). In the training of cybersecurity experts, Castro-León and Rendón-Burgos (2021) indicate that it is crucial to recognize the need for adequate training for future professionals in computer science careers. This is especially relevant given the drastic change that the internet has caused in several sectors, of which communications has been one of the most affected. Therefore, studying cybersecurity practically is an effective way to develop expertise in the student, as it allows them to develop technical skills and adapt to dynamic

scenarios. This also deepens their understanding of vulnerabilities, improves awareness of the importance of cybersecurity, and prepares them for the world of work by demonstrating directly applicable skills, complying with the human-based cybersecurity approach (Grobler *et al.*, 2021; Marble *et al.*, 2015; Likewise, it promotes professional ethics by conducting tests in an ethical and legal manner, which promotes responsibility and integrity in the handling of sensitive information.

For all of the above, the development of EthkLab was considered pertinent to strengthen the ethical *hacking skills* of the students of the Computer Systems Engineering degree at the Tecnológico Nacional de México campus Progreso. This low-cost technological development can perform the same functions as laboratories at other institutions, although it should be noted that the initial questions about its effective performance must be verified, as was done in this study.

In this specific case, although the preliminary results indicate that EthkLab can be used in a training course, it is important to consider some aspects of improvement based on the final perception of a minority of the participants. Aspects such as understanding the comprehensive internship process, the complexity of the integration of EthkLab with personal computing equipment, and the overall satisfaction experience did not reach 80% acceptance, suggesting the need to address these aspects in greater depth. However, other indicators support the hypothesis that the practices included in EthkLab can significantly improve students' skills.

Conclusions

EthkLab emerges as an innovative solution in the field of cybersecurity education, providing a Raspberry Pi 4-based physical lab that integrates simulated ethical *hacking* and *pentesting environments*. Although in its early stages, this approach offers users a practical and realistic environment for skill development, as it allows for the safe application and exploration of techniques and strategies related to ethical *hacking*.

Although some tests did not reach 100% success, the results obtained reveal strong potential for fine-tuning and perfecting operational details. This initial data provides valuable insights and experiences that can be used to optimize lab effectiveness and improve the success rate with participating students. The flexibility and versatility inherent in EthkLab, due to its construction with low-cost and modular devices, allows for continuous adjustment

and improvement, providing the opportunity to address specific areas that require additional attention. Finally, the feedback collected during these initial tests serves as a valuable resource for future refinement of the system, paving the way for more effective deployment and obtaining even more robust results in future iterations.

Future lines of research

This study has yielded encouraging results on the feasibility and acceptance of a controlled cyber environment (EthkLab) for learning *pentesting* and ethical *hacking* using low-cost devices, specifically the Raspberry Pi 4 set of cards. However, there are still areas of research to be explored to improve both the performance and effectiveness of these environments. Among the proposals for future lines of research, the following are recommended:

1. Low-cost cyber environment optimization: Extensive research is suggested to optimize the low-cost cyber environment through different configurations and *software systems*, as well as evaluation of different *hardware*. Although the use of Raspberry Pi 4 cards has proven to be effective, it is important to explore other *hardware options* that can offer greater computing power at a similar price. Therefore, the use of Jetson Nano cards or even mini-PCs with 64-bit architecture could be considered. Investigating these alternatives could provide insights into how to improve the processing capacity and efficiency of the learning environment. Additionally, the possibility of replacing preconfigured operating systems, such as Kali Linux, could be evaluated with the option of manually configuring the lab with minimalist operating systems that include only the tools necessary for the test scenarios. This approach could allow greater control over the *software* used and optimize system performance, as well as offer a more personalized learning experience.
2. Quantitative and qualitative evaluation of learning with EthkLab: It is proposed to carry out progressive evaluations of students with defined plans in the field of ethical *hacking* and *pentesting* as part of another study, with special emphasis on the development and evolution of the acquired skills. Likewise, it is suggested to carry out a comprehensive evaluation of learning using EthkLab, addressing both quantitative and qualitative aspects. This research would seek to fully understand the impact and effectiveness of EthkLab as a teaching tool in the field of cybersecurity,

through the collection and analysis of quantitative data on performance and learning outcomes, as well as qualitative data that investigates the experience. and user perception. The objective is to provide a comprehensive and informed view on the use of EthkLab as an educational resource to improve the quality and effectiveness of teaching in this field.

Acknowledgments

The authors thank the Tecnológico Nacional de México for the financial financing of this project, which was carried out from January 1, 2023, to December 31, 2023. They also thank the students of the seventh semester, generation of 2020, of the Computer Systems Engineering degree from the Tecnológico Nacional de México campus Progreso, and professor Edgar Alejandro Sagundo Duarte for his collaboration and the class time given for the tests carried out.

References

Arreola-García, A. (2019). Desafíos a las estrategias de ciberseguridad en América. *Revista del Centro de Estudios Superiores Navales*, *40*(4), 25–53.

Castro-León, G. K. y Rendón-Burgos, C. E. (2021). *Creación de un entorno virtual de aprendizaje para un laboratorio de enseñanza de seguridad informática en carreras técnicas* (trabajo de grado). Universidad de Guayaquil. http://repositorio.ug.edu.ec/handle/redug/57097

Fuentes-Penna, A. F., Gómez-Cárdenas, R. y González-Ibarra, J. de D. (2023). La Ciberseguridad en México y los derechos humanos en la era digital. *Espacios Públicos*, *24*(61), 110–130.

Grobler, M., Gaire, R. and Nepal, S. (2021). User, Usage and Usability: Redefining Human Centric Cyber Security. *Frontiers in Big Data*, *4*. https://www.frontiersin.org/articles/10.3389/fdata.2021.583723

Legg, P., Mills, A. and Johnson, I. (2023). Teaching Offensive and Defensive Cyber Security in Schools using a Raspberry Pi Cyber Range. *Journal of The Colloquium for Information Systems Security Education*, *10*(1), Article 1. https://doi.org/10.53735/cisse.v10i1.172

Marble, J. L., Lawless, W. F., Mittu, R., Coyne, J., Abramson, M. and Sibley, C. (2015). The Human Factor in Cybersecurity: Robust & Intelligent Defense. In S. Jajodia, P.

Shakarian, V. S. Subrahmanian, V. Swarup and C. Wang (eds.), *Cyber Warfare: Building the Scientific Foundation* (pp. 173–206). Springer International Publishing. https://doi.org/10.1007/978-3-319-14039-1_9

Martínez-Luengo, D. (2021). Anonimato y Pentesting con Raspberry Pi. http://e-spacio.uned.es/fez/view/bibliuned:master-ETSInformatica-CBS-Dmartinez

Muñoz-Martínez, M. (2020). Políticas educativas e incorporación de las TIC en la educación superior mexicana. *Revista Digital Universitaria*, *21*(6). https://biblat.unam.mx/es/revista/revista-digital-universitaria/articulo/politicas-educativas-e-incorporacion-de-las-tic-en-la-educacion-superior-mexicana

Oh, S. K., Stickney, N., Hawthorne, D. and Matthews, S. J. (2020). *Teaching Web-Attacks on a Raspberry Pi Cyber Range*. Proceedings of the 21st Annual Conference on Information Technology Education, 324–329. https://doi.org/10.1145/3368308.3415364

Pearson, B., Luo, L., Zou, C., Crain, J., Jin, Y. and Fu, X. (2020). Building a Low-Cost and State-of-the-Art IoT Security Hands-On Laboratory. En A. Casaca, S. Katkoori, S. Ray and L. Strous (eds.), *Internet of Things. A Confluence of Many Disciplines* (pp. 289–306). Springer International Publishing. https://doi.org/10.1007/978-3-030-43605-6_17

Raspberry Pi Ltd. (s. f.). Buy a Raspberry Pi 400 Personal Computer Kit. Raspberry Pi. https://www.raspberrypi.com/products/raspberry-pi-400/

Salazar-Mata, J. M., Cruz-Navarro, C., Balderas-Sánchez, A. V. y Díaz-Uribe, H. F. (2021). La seguridad informática en las instituciones de educación superior. TECTZAPIC: *Revista Académico-Científica*, *7*(2), 72–79.

Torres-Knight, R. R. T. y Méndez-Morales, O. A. M. (2023). Esfuerzo dentro del estado de Chihuahua, México en materia de ciberseguridad. Informática y Derecho. *Revista Iberoamericana de Derecho Informático*, *13*(2.ª época).

Velasco-Arellanes, F. J., Vera-Noriega, J. Á. y Durazo-Salas, F. F. (2020). La educación universitaria pública mexicana en el libre mercado: necesidades, ausencias y confusiones en su mejoramiento. *Voces y Silencios. Revista Latinoamericana de Educación*, *11*(2). https://doi.org/10.18175/VyS11.2.2020.9

Yamin, M. M., Katt, B. and Gkioulos, V. (2020). Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, *88*, 101636. https://doi.org/10.1016/j.cose.2019.101636

Zimmermann, V. and Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Contribution Role	Author(s)
Conceptualization	Holzen Atocha Martínez García (main).
Methodology	Holzen Atocha Martínez García (main).
Software Installation	Holzen Atocha Martínez García (main).
Validation	Holzen Atocha Martínez García (main). Enrique Camacho Pérez (same). Ligia Beatriz Chuc Us (same).
Formal Analysis	Holzen Atocha Martínez García (main).
Investigation	Holzen Atocha Martínez García (same). Enrique Camacho Pérez (same). Ligia Beatriz Chuc Us (same).
Resources	Holzen Atocha Martínez García (same). Enrique Camacho Pérez (same).
Data curation	Enrique Camacho Pérez (same). Ligia Beatriz Chuc Us (same).
Writing - Preparation of the original draft	Holzen Atocha Martínez García (main).
Writing - Review and editing	Holzen Atocha Martínez García (main). Enrique Camacho Pérez (same)
Display	Holzen Atocha Martínez García (same). Enrique Camacho Pérez (same).
Supervision	Holzen Atocha Martínez García (main). Edgar Alejandro Sagundo Duarte (supporting).
Project Management	Holzen Atocha Martínez García (main).
Fund acquisition	Holzen Atocha Martínez García (main). Enrique Camacho Pérez (same). Ligia Beatriz Chuc Us (same).