Development of Penetration Testing Learning Module Based on the ADDIE Model

Ahmad Anwary Adzirudin, Nanang Trianto, Dimas Febriyan Priambodo
and Septia Ulfa Sunaringtyas
Department of Cyber Security Engineering, National Cyber and Crypto Polytechnic, Bogor, West Java, Indonesia

Keywords: Penetration Testing, Learning Module, ADDIE Model, Learning Management System, Virtual Laboratory.

Abstract: This study outlines the development of a penetration testing learning module based on the ADDIE instructional design model. The module combines a Learning Management System (LMS) and a virtual laboratory environment (OVA) to support both theoretical and practical cybersecurity education. Driven by the rising number of cyberattacks and the shortage of skilled professionals, the module aligns with Indonesia's Cybersecurity Testing Competency Standards (SKKNI) and includes seven modules covering key stages of penetration testing. A mixed-method approach was used: qualitative methods for needs analysis and instructional design, along with quantitative assessments through the Content Validity Index (CVI) and User Acceptance Testing (UAT). Expert validation yielded a perfect S-CVI score of 1.00, indicating high content relevance. The implementation was evaluated via UAT to gather user feedback on perceived usefulness and ease of use. The acceptance score was 92.17%, classified as highly accepted by participants. This demonstrates that the developed module effectively enhances technical skills in system penetration testing and can serve as a structured reference for penetration testing education.

1 INTRODUCTION

Technological developments bring benefits to various sectors, but they also bring security risks in the form of cyber attacks. Cyber attacks have increased significantly in organizations every week, with an average of 1,876 attacks in the third quarter of 2024 (Fa'izi, 2024). Cyber attacks can be triggered by internal factors such as weak security systems, lack of system updates, careless user behavior, and limited human resource (HR) competence (Azizah et al., 2024). Weak security systems can be strengthened by mitigating system vulnerabilities from the outset through system penetration testing. System penetration testing is a technique for finding weaknesses in a system using the same methods as attackers. Systems are tested by ethical hackers to help companies understand their security needs (Kozel & Drozdova, 2024). In the 2024 ID SIRTII Report, the BSSN Cyber Security Operations Directorate conducted system penetration testing on 131 agencies. A total of 1,931 security vulnerabilities were found in 462 applications through system penetration testing activities (Id-SIRTII /CC, 2024).

In conducting system penetration testing, the Indonesian National Work Competency Standards (SKKNI) for Cyber Security Testing serve as a guide for organizations in both the government and private sectors. The SKNNI Cyber Security Testing Standards have the primary objective of providing information on the results of cyber security testing for organizational security improvements (Ida Fauziyah, 2022). Although competency standards are available, cybersecurity human resource capacity in Indonesia is still very limited. The Chair of the Indonesia Cyber Security Forum (ICSF) stated that Indonesia requires 10,000 cybersecurity experts annually (KKIP, 2023). While system penetration testing plays a role in enhancing cybersecurity, not all organizations recognize the importance of developing cybersecurity human resources. The demand for cybersecurity human resources is increasing, while the number of cybersecurity experts remains limited. Therefore, there is a need to enhance human resources through cybersecurity training with relevant curricula (Kunci, 2025).

Anwary Adzirudin, A., Trianto, N., Febriyan Priambodo, D. and Ulfa Sunaringtyas, S.
Development of Penetration Testing Learning Module Based on the ADDIE Model.
DOI: 10.5220/0014266100004928
Paper published under CC license (CC BY-NC-ND 4.0)
In *Proceedings of the 1st International Conference on Research and Innovations in Information and Engineering Technology (RITECH 2025)*, pages 108-113
ISBN: 978-989-758-784-9
Proceedings Copyright © 2025 by SCITEPRESS – Science and Technology Publications, Lda.

Previous studies have developed a learning product. Research (Dalimunthe, Affandi, & Suryanto, 2021) shows that the R&D method with the ADDIE approach produces modules with an average score above 89%. The product has met the criteria for clarity, relevance, and ease of use. Another study (Zhang & Liu, 2023) discusses the successful design and implementation of virtual laboratories integrated into a virtual experiment learning management platform, which met functional requirements and positively impacted learning outcomes, as evaluated by learners over two years. Additionally, study (Li, 2015) demonstrated that developing learning modules for system penetration testing through practical exercises can reinforce theoretical concepts and technical skills. Another study (Teerakanok, Rassameeroj, Khurat, & Visoottiviseth, 2022) shows that participants successfully learned system penetration testing skills in depth through practical exercises in a virtual laboratory. The research results provide recommendations for conducting learning based on system penetration testing practical exercises.

In this study, a system penetration test learning module will be created using the ADDIE model. The ADDIE model consists of five stages are analysis, design, development, implementation, and evaluation (Adolph, 2016). The stages in the ADDIE model will serve as the foundation for creating an LMS-based learning product. The LMS will be used as a learning platform that provides learning materials online (Mustapha et al., 2023). A virtual laboratory will be used as a simulation tool for conducting system penetration testing practices. Participants will identify security vulnerabilities in the provided server (Mahtuf, Hatta, & Wihidiyat, 2019). The researcher will also conduct functional testing to assess the suitability of the developed learning medium with the Learning Technology Development Unit. In this study, the SKKNI Cybersecurity Testing Standards will serve as a reference for developing the system penetration testing learning module (Ida Fauziyah, 2022).

This study aims to develop a structured system penetration testing learning module for conducting system penetration testing. In addition, the developed product will be evaluated to determine the level of participant acceptance of the learning module through User Acceptance Testing (). The results of this study are expected to contribute to the community's development of competencies in the field of system penetration testing.

2 METHODOLOGY

This study uses a Research and Development (R&D) methodology aimed at producing a prototype learning module for penetration testing. The R&D process is structured using the ADDIE model, an instructional design framework consisting of five sequential phases: analysis, design, development, implementation, and evaluation. Each phase provides a systematic process for identifying learner needs, designing instructional content, developing media, testing implementation, and evaluating outcomes. This study integrates qualitative and quantitative approaches. The qualitative approach is used to collect data related to instructional needs and design requirements for the penetration testing learning module. The quantitative approach is applied to evaluate the usability and acceptance of the module developed by learners. The final product includes a Learning Management System (LMS) containing theoretical content and a virtual laboratory environment based on OVA that facilitates practical penetration testing exercises.

3 RESULTS

3.1 Analysis

The analysis stage was conducted to identify the needs and issues that form the basis for the development of the system penetration testing learning module. Based on interviews with the Learning Technology Development Unit, it was found that the development of web-based learning facilities is urgently needed to support the achievement of competencies in the field of cybersecurity. The interviewees stated that facilities such as LMS and virtual laboratories can enhance participants' abilities and skills through an outcome-based learning approach. The development of learning media in the field of system penetration testing is considered important to support effective learning processes. Several elements must be fulfilled in the development of learning media, including:

- A clear curriculum foundation;
- Consideration of participant characteristics to align with learning objectives;
- Establishment of procedures for using learning materials;
- Evaluation aligned with content and learning objectives.

- Documentation of all required configurations and credentials
- Utilization of resources according to needs

3.2 Design

The learning media design is intended to facilitate participants' understanding of concepts and hone their technical skills through a systematic learning process. The learning flow in this media is illustrated in Figure 1.

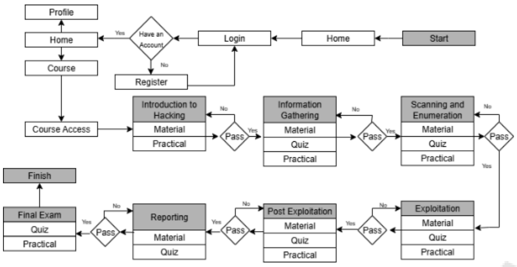

Figure 1: Participant Interaction with Learning Media.

Figure 1 illustrates the flow of participant interaction with LMS-based learning media and the OVA laboratory. The process begins on the main page, where participants can register or log in to the system. After successfully logging in, participants are directed to the course page to access the system penetration testing learning module. The material is presented in text and image form, while practical exercises are carried out using the OVA laboratory, which can be downloaded via the provided link. Before conducting practical exercises, participants are given preparatory instructions to set up the virtual laboratory. Participants can only proceed to the next module after passing the quiz and completing the practical exercises in the previous module. A final exam is conducted to comprehensively assess participants' understanding of theory and practical skills. For participants who have not completed the practical exercises, explanatory videos will be provided as additional learning materials.

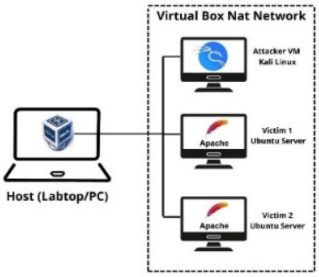

Figure 2: Virtual Laboratory Penetration Testing Topology.

Figure 2 shows the virtual laboratory topology used in this study. The environment is built on a VirtualBox NAT network consisting of one attacker machine (Kali Linux) and two victim machines (Ubuntu Server). This configuration enables participants to conduct penetration testing activities, including information gathering, scanning, exploitation, and post-exploitation, in a controlled and isolated environment without affecting external networks.

3.3 Development

The development stage aims to turn the learning design into a usable learning product. Learning media is developed based on the interaction design and learning flow that have been designed, with the Learning Management System (LMS) as the main access point and the OVA laboratory as the practical facility. The learning module content consists of seven main sections are introduction to hacking, information gathering, scanning and enumeration, exploitation, post-exploitation, reporting, and final exam. Each module includes theoretical material and practical scenarios aligned with the competency units in the SKKNI Cyber Security Testing Standards. Practical exercises are designed to train participants in using various tools, such as Nmap, Nikto, Hydra, and Metasploit, and include activities ranging from network mapping, access exploitation, to post-exploitation, such as backdooring and web defacement. The details of the materials and practical scenarios for each module are presented in Table 1 below.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

Table 1: Practical Materials and Scenarios.

Module	Material Requirements	Practical Scenario
Introduction to Hacking	Introduction to Hacking, Terminology in Penetration Testing, Ethics in Penetration Testing, Methodologies	Kali Linux installation
Information Gathering	Concept of Information Gathering, Passive Information Gathering Techniques, Active Information Gathering Techniques, Standard Target Identification	Using Nmap for network and open port mapping, identifying main service names, identifying versions, and used ports

Module	Material Requirements	Practical Scenario
	Tools, and OS Fingerprinting	
Scanning and Enumeration	Basics of Metasploit Framework, Fundamentals of Scanning & Enumeration, Scanning with Nessus, OpenVAS, and Nikto, Enumeration	Running Nikto to scan for vulnerabilities, FTP anonymous enumeration, and Enumeration using Metasploit scanner
Exploitation	Fundamentals of Exploitation, Common Vulnerabilities and Exposure (CVE), Exploits and Attacks using Metasploit, Using Hydra	Running Hydra for brute force, Exploiting server access using SSH
Post Exploitation	Privilege Escalation, Backdooring Techniques, Persistence Techniques	Running a backdoor, Executing persistence, Post-exploitation (web defacement)
Reporting	Writing a Penetration Testing Report, Common Vulnerability Scoring System (CVSS), Sample Penetration Test Report	Writing the report document
Final Exam	All materials learned in previous chapters	System identification, Mapping & scanning, Directory enumeration, Login exploitation, Post-exploitation with backdoor and web defacement

3.4 Implementation

The implementation stage was carried out by conducting trials of the developed system, penetration testing learning module with a total of 40 participants. These participants were selected based on specific criteria, namely individuals who already possessed basic knowledge of networking and Linux system administration, to ensure they were adequately prepared for the technical content delivered in the module.

The implementation lasted for one week, during which participants engaged in structured learning activities through a Learning Management System (LMS) and completed hands-on practical exercises using the provided OVA-based virtual laboratory. Each day, participants accessed theoretical materials and carried out penetration testing tasks according to the learning flow designed in the module.

Throughout the implementation, participants progressed sequentially through the seven modules, ranging from introductory concepts to the final exam by completing quizzes and practical assignments. Progression to subsequent modules was gated by the completion of both theory and practice components from previous modules. The implementation phase also involved continuous technical support and monitoring to ensure the module ran as intended and that learners could complete the practical tasks without significant obstacles.

3.5 Evaluation

The evaluation of the system penetration testing learning module was carried out through a User Acceptance Test (UAT) involving participants who had completed all modules and practical activities. The purpose of this evaluation was to assess the level of user satisfaction and acceptance of the developed product from the perspective of its usefulness and ease of use.

The assessment employed two main indicators are Perceived Usefulness and Perceived Ease of Use, both measured using a 5-point Likert scale. In this scale, a score of 1 indicates Strongly Disagree, while a score of 5 indicates Strongly Agree. The Perceived Usefulness indicator was intended to evaluate the extent to which users felt that the learning module helped facilitate their learning process and improve their skills in conducting system penetration testing.

Based on the UAT survey results, responses were overwhelmingly positive. Almost all respondents gave a score of 5 for the following statements are the module helped them perform penetration testing more quickly (97%), improved their overall performance (93.9%), and made the learning process more productive (81.8%). Additionally, 87.9% reported that the module improved their understanding of the penetration testing stages, while 81.8% agreed that penetration testing became easier to carry out with the help of the module. These results suggest that the

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS

product provides substantial practical benefits for developing technical competence.

As for Perceived Ease of Use, the responses were also highly favorable. A total of 90.9% of participants stated that the module was easy to operate, 87.9% rated the interface as user-friendly, and 84.8% encountered minimal technical issues while using the system. Furthermore, 81.8% appreciated the flexibility offered by the module, and 78.8% felt that it supported the development of their practical skills.

In addition to the UAT survey, quantitative data was collected from practical exercises. All 40 participants (100%) successfully completed all learning modules, indicating that the design and sequence of tasks could be completed within the given time frame. The average completion time for each module ranged from 45 to 110 minutes, with the exploitation and post-exploitation stages taking the longest. These results indicate that participants were able to effectively achieve theoretical and practical learning objectives.

4 DISCUSSION

This study shows that the penetration testing learning module developed using the ADDIE instructional design model can effectively improve participants' theoretical knowledge and practical skills in the field of cybersecurity. The Content Validity Index (CVI) achieved a perfect S-CVI score of 1.00, confirming that all materials and assessments are highly relevant and aligned with the SKKNI cybersecurity testing competency standards. The one-week implementation involving 40 participants further validated the effectiveness of the module, as the structured learning flow through seven modules improved participants' ability to perform complex penetration testing tasks. UAT results also supported this effectiveness, showing positive user feedback and successful completion of the learning process without major issues.

Compared to the study by (Teerakanok et al., 2022), which focused on qualitative experiences using OVA-based laboratories, this study applied a structured instructional design and incorporated quantitative metrics, making the modules more standardized and measurable. Similar international initiatives, as described by (Li, 2015; Zhang & Liu, 2023), also highlight the effectiveness of integrating penetration testing training into virtual laboratories and LMS platforms. However, this study expands on their findings by aligning the module with Indonesian SKKNI standards, ensuring national relevance while maintaining global comparability.

Despite these advantages, several limitations must be acknowledged. The study was conducted in a relatively short period and involved participants who already had prior networking and Linux knowledge, which may not fully represent a broader target audience such as beginners or those from non-technical backgrounds.

Future module development should consider upgrading the LMS with more interactive features to increase learner engagement and flexibility. Examples include gamification elements such as points, badges, and leaderboards to motivate learners, adaptive learning paths that adjust to learners' skill levels, and real-time feedback mechanisms to reinforce the learning experience. These features will make the platform more dynamic and sustainable for diverse learners while remaining aligned with national standards.

5 CONCLUSIONS

The development of the penetration testing learning module based on the ADDIE instructional design model has significantly improved participants' competencies in system penetration testing. The CVI results confirmed the strong alignment of the module's theoretical content, practical exercises, and assessments with the SKKNI Cybersecurity Testing competency standards. The one-week implementation with 40 participants showed that the module's structured approach effectively guided learners through seven modules, enabling them to handle complex penetration testing tasks with improved confidence and technical proficiency. This outcome was also reflected in the UAT results, where over 90% of participants acknowledged that the module enhanced their skills, productivity, and understanding of penetration testing processes. Overall, the learning module consistently strengthens cybersecurity competencies and has the potential to be adopted as a scalable and standardized training solution to address the shortage of skilled cybersecurity professionals in Indonesia.

ACKNOWLEDGEMENT

The authors would like to thank the State Cyber and Cryptography Polytechnic for their support in providing facilities and academic guidance during this research. We would also like to thank the reviewers for their valuable input, which has improved the quality of this paper.

REFERENCES

Adolph, R. M. (2009). Instructional design: The ADDIE approach. Springer. https://doi.org/10.1007/978-0-387-09506-6

Azizah, S., Ula, Z. N., Mutiara, D., & Prameswari, M. P. (2024). Keamanan siber sebagai fondasi pengembangan aplikasi keuangan mobile: Studi literatur mengenai cybercrime dan mitigasinya. Akuntansi dan Teknologi Informasi, 17(2), 221–237. https://doi.org/10.24123/jati.v17i2.6409

Bertagnolli, C. (2011). Perceived usefulness, perceived ease of use, and user acceptance of information technology. Delle vicende dell'agricoltura Ital. Studi e note di C. Bertagnolli, 13(3), 319–340.

Chai, C. S., Hipiny, I., & Ujir, H. (2023). User acceptance testing (UAT) of self-service checkout kiosks: A case study in E-Mart Tabuan Jaya, Kuching, Malaysia. Proceedings of the 2023 IEEE 7th International Conference on Information Technology, Information Systems and Electrical Engineering (ICITISEE), 6–11.

Creasey, J. (2017). A guide for running an effective penetration testing programme. Crest, (April), 1–64.

Dalimunthe, A., Affandi, M., & Suryanto, E. D. (2021). Pengembangan modul praktikum teknik digital model ADDIE. Jurnal Teknologi Informasi & Komunikasi Dalam Pendidikan, 8(1), 17. https://doi.org/10.24114/jtikp.v8i1.26777

Fa'izi, M. B. N. (2024). Serangan siber global melonjak 75% di Q3 2024. Cyberhub. https://cyberhub.id/berita/serangan-siber-global-melonjak-di-2024

Fauziah, I., Situmorang, R., & Suprayekti. (2022). Pengembangan modul hypercontent untuk mata diklat kode etik dan disiplin pegawai BPK RI. Jurnal Pembelajaran Inovatif, 5(2), 42–49.

Hadi, A. P., Rudjiono, R., & Zainudin, A. (2024). ADDIE model dalam pengembangan media informasi untuk menumbuhkan minat peserta. Go Infotech: Jurnal Ilmiah STMIK AUB, 30(1), 20–27.

Id-SIRTII/CC. (2024). Lanskap keamanan siber Indonesia. Id-SIRTII/CC BSSN, 1–141.

Kementerian Ketenagakerjaan Republik Indonesia. (2022). Standar kompetensi kerja nasional Indonesia bidang uji keamanan siber (Vol. 01, pp. 1–49).

KKIP. (2023). Ulasan ringkas kajian KKIP tahun 2022: Kajian strategis pembangunan industri pertahanan bidang siber dan ekosistemnya. Komite Kebijakan Industri Pertahanan. https://www.kkip.go.id/2023/03/15/ulasan-ringkas-kajian-kkip-tahun-2022-kajian-strategis-pembangunan-industri-pertahanan-bidang-siber-dan-ekosistemnya/

Kozel, V. M., & Drozdova, I. E. A. (2024). Research of penetration testing methods. Vestnik Kherson National Technical University, 3(90), 221–227. https://doi.org/10.35546/kntu2078-4481.2024.3.28

Li, C. (2015). Penetration testing curriculum development in practice. Journal of Information Technology Education: Innovations in Practice, 14(1), 85–99. https://doi.org/10.28945/2189

Machmudi, M. A., Wahyudiono, S., & Susilo, G. (2023). Analisis dan rancang bangun e-learning dengan metode ADDIE model. Go Infotech: Jurnal Ilmiah STMIK AUB, 29(2), 226–232.

Mustapha, A. M., Zakaria, M. A. Z. M., Yahaya, N., Abuhassna, H., Mamman, B., Isa, A. M., & Kolo, M. A. (2023). Students' motivation and effective use of self-regulated learning on learning management system Moodle environment in higher learning institution in Nigeria. International Journal of Information and Education Technology, 13(1), 195–202. https://doi.org/10.18178/ijiet.2023.13.1.1796

NIST. (2021). Technical guide to information security testing and assessment (SP 800-115). Gaithersburg, MD: National Institute of Standards and Technology.

OWASP Foundation. (2021). Penetration testing methodologies. OWASP Web Security Testing Guide. https://owasp.org/www-project-web-security-testing-guide/latest/

Pramono, G. J., & Napitulu, T. A. (2022). User acceptance in non-profit organization applications: The role of intention to use, perceived usefulness, and community commitment. ITEJ (Information Technology Engineering Journals), 7(1), 53–76.

Shahriar, H., et al. (2023). Technology adoption model-based comparison of clinical trial software. International Journal of Applied Research in Public Health Management, 8(1), 1–24.

Shanley, A., & Johnstone, M. N. (2015). Selection of penetration testing methodologies: A comparison and evaluation. Australasian Information Security Management Conference (AISM), 65–72.

Shrestha, N. (2012). Security assessment via penetration testing: A network and system administrator's approach (Master's thesis). University of Oslo.

Teerakanok, S., Rassameeroj, I., Khurat, A., & Visoottiviseth, V. (2022). Lessons learned from penetration testing hands-on training during COVID-19 pandemic. 6th International Conference on Information Technology, InCIT 2022, 368–373. https://doi.org/10.1109/InCIT56086.2022.10067755

Wang, F., & Sahid, S. (2024). Content validation and content validity index calculation for entrepreneurial behavior instruments among vocational college students in China. Multidisciplinary Reviews, 7(9).

Yusoff, M. S. B. (2019). ABC of content validation and content validity index calculation. Education in Medicine Journal, 11(2), 49–54.

Yusron, M. (2025). Pembinaan peningkatan kapasitas SDM tim tanggap insiden siber pemerintah daerah Provinsi Banten. Jurnal Cahaya Nusantara, 1(2), 86–92. https://jurnal.cahayapublikasi.com/index.php/jcn/article/view/87