JMM (Jurnal Masyarakat Mandiri)
http://journal.ummat.ac.id/index.php/jmm
Vol. 9, No. 1, Februari 2025, Hal. 978-989
e-ISSN 2614-5758 | p-ISSN 2598-8158
Crossref : https://doi.org/10.31764/jmm.v9i1.28646

ENHANCING VOCATIONAL SCHOOL STUDENTS' COMPETENCE IN OPERATING SYSTEM SECURITY THROUGH HARDENING TRAINING TO IMPROVE AWARENESS OF CYBER THREATS

Achamd Sutanto[1*], Lukmanul Khakim[2], Eko Budi Hartono[3], M. Khoirul Umam[4]
[1,2,3]D3 Teknik Komputer, Politeknik Harapan Bersama, Indonesia
[4]D4 Bisnis Digital, Politeknik Siber Cerdika Internasional, Indonesia
achmadsutanto@gmail.com

ABSTRACT

Abstrak: Keamanan sistem operasi merupakan elemen krusial dalam melindungi perangkat digital dari ancaman siber. SMK Negeri 2 Tegal, yang memiliki jurusan Teknik Jaringan Komputer dan Telekomunikasi, menghadapi tantangan dalam meningkatkan kompetensi siswa dalam bidang keamanan sistem operasi, khususnya dalam teknik hardening. Tujuan pengabdian ini adalah untuk meningkatkan keterampilan siswa dalam mengamankan sistem operasi Windows dan Linux melalui pelatihan hardening. Metode yang digunakan mencakup seminar interaktif dan praktik langsung di laboratorium komputer di SMK Negeri 2 Tegal dengan 33 siswa kelas XI jurusan Teknik Jaringan Komputer dan Telekomunikasi (TKTJ). Evaluasi dilakukan melalui pre-test dan post-test untuk mengukur peningkatan pemahaman dan keterampilan siswa. Hasil pengabdian menunjukkan peningkatan signifikan dalam pemahaman siswa, dengan nilai rata-rata post-test meningkat sebesar 22.7%, dari 66 menjadi 81. Keunikan pengabdian ini terletak pada pendekatan yang menggabungkan teori dan praktik langsung, serta modul pelatihan yang disesuaikan dengan kebutuhan siswa. Sebagai rekomendasi, disarankan untuk mengadakan pelatihan lanjutan dan mengintegrasikan materi keamanan sistem operasi ke dalam kurikulum untuk meningkatkan kualitas pendidikan, kesiapan siswa menghadapi dunia kerja, dan ketahanan digital di dunia pendidikan.

Kata Kunci: Keamanan Sistem Operasi; Hardening; Pelatihan Keamanan Siber; Pendidikan Vokasi.

Abstract: *Operating system security is a crucial element in protecting digital devices from cyber threats. SMK Negeri 2 Tegal, with its Computer Network and Telecommunications program, faces challenges in improving students' competencies in operating system security, particularly in hardening techniques. This community service aims to enhance students' skills in securing Windows and Linux operating systems through hardening training. The method employed includes interactive seminars and hands-on practice in the computer laboratory at SMK Negeri 2 Tegal, envolving 33 students from the eleventh grade of the Computer Network Engineering and Telecommunications (TKTJ) program. Evaluation is carried out through pre-tests and post-tests to measure the improvement in students' understanding and skills. The results show a significant increase in students' understanding, with the average post-test score rising by 22.7%, from 66 to 81. The uniqueness of this service lies in the approach that combines theory and hands-on practice, along with training modules tailored to students' needs. As a recommendation, it is advised to conduct further training and integrate operating system security into the curriculum to enhance educational quality, students' readiness for the workforce, and digital resilience in education.*

Keywords: *Operating System Security; Hardening; Cybersecurity Training; Vocational Education*

Article History:
Received: 19-12-2024
Revised : 17-01-2025
Accepted: 21-01-2025
Online : 15-02-2025

A. INTRODUCTION

The worldwide landscape of cyber threats is changing swiftly in tandem with technological progress and greater digital connectivity. This trend is marked by the increasing complexity and sophistication of cyberattacks, which frequently employ more coordinated and weaponized methods (Radoglou-Grammatikis et al., 2023; Wiratama, 2023). Cyber threats are now a major challenge not only in the technical realm, but also in the socio-economic and political aspects, which require a multidimensional approach in mitigation efforts. Ransomware attacks, for example, have evolved from mere data encryption to data exfiltration and espionage, thereby demanding more complex and integrated security solutions (McIntosh et al., 2024; Riggs et al., 2023). Furthermore, the impact of cyber threats also varies by geography, often correlating with a region's level of socioeconomic development. These threats also increasingly involve social aspects, such as the spread of misinformation and cyberbullying, which adds to the complexity of the problem (Chen et al., 2023; Kursuncu et al., 2023). Threats to the global economy and cyber resilience are becoming increasingly urgent, especially in the trade and supply chain sectors affected by AI-driven cyberattacks (Osman & El-Gendy, 2024).

SMK Negeri 2 Tegal, especially in the Computer Network and Telecommunication Engineering department, faces challenges in improving student competence in operating system security. Although this department has focused on mastering computer and network technology, materials related to strengthening operating system security through hardening techniques are still not a top priority in the curriculum. As a result, students do not have adequate understanding or practical skills to face the challenges of the cyber world, especially in managing and securing Windows and Linux operating systems (Sutanto, 2024). Limited resources and a lack of structured training modules exacerbate the gap in student competency in cybersecurity. Previous research has shown that structured practicum-based training can improve students' skills in operating system security (Soares et al., 2023). This emphasises the importance of training that is more integrated with the curriculum to improve students' readiness to face the increasingly complex demands of the world of work.

The integration of operating system security training into the vocational education curriculum is essential to prepare students for the challenges of the cyber world. Research shows that education that combines theoretical learning with hands-on practice can result in a deeper understanding of the topic (Allison, 2023; Laundon et al., 2023). In addition, the application of active learning methods, such as group discussions and simulations, can help students apply acquired knowledge in real-world situations (Jerman Blažič & Jerman Blažič, 2022). Research has also shown that simulation-based learning and the use of interactive learning tools, such as videos and serious games, can improve students' understanding of more complex concepts in

cybersecurity (Laundon et al., 2023). Modular training programs tailored to industry needs, such as those applied to the maritime sector, have proven effective in preparing students for specific cybersecurity challenges (Affia et al., 2023; Oruc et al., 2024). In the context of vocational education, the integration of such training enables students to develop the technical and soft skills needed in the industrialised world (Onyango & Kelonye, 2022). Therefore, a holistic curriculum approach that covers various aspects of cybersecurity is highly relevant in preparing the younger generation to deal with increasingly complex threats (Affia et al., 2023; Safitra et al., 2023).

To overcome the problems faced by SMK Negeri 2 Tegal, a comprehensive training program on operating system hardening was designed. The training included the creation of a learning module tailored to students' level of understanding, teaching techniques for securing Windows- and Linux-based operating systems, and hands-on laboratory practice. This approach combines theory and practice to give students hands-on experience in applying operating system security measures. The training concludes with a real simulation-based evaluation to measure the effectiveness of the program and students' readiness to face increasingly dynamic cyber threats (Osman & El-Gendy, 2024).

The main objective of this activity is to improve the competence of SMK Negeri 2 Tegal students in the field of operating system security so that they are better prepared to face the increasingly complex demands of the world of work. In addition, this activity aims to contribute to the development of a more comprehensive vocational education curriculum, especially by integrating operating system hardening material as an integral part of learning, so that students can face the increasingly high demands of cyber security in the industrial world.

B. METHOD

This community service activity consists of two main groups of participants: lecturers and students. The primary role of the lecturers is to provide training and assistance to students of SMK Negeri 2 Tegal regarding operating system security through hardening techniques on Windows and Linux. This includes counseling on the importance of operating system security and how hardening techniques can mitigate potential cyber threats. Lecturers present both theoretical and practical materials related to this topic, utilizing a blended learning approach that combines theoretical sessions with hands-on laboratory practice. They also provide direct assistance during practical sessions and discuss the application of security in the industrial context.

Students participate as facilitators in the training, focusing on enhancing cybersecurity literacy among their peers. They assist during practical sessions in the laboratory and offer technical support while implementing hardening techniques. Additionally, students actively monitor and evaluate

their peers' progress in applying security techniques on both Windows and Linux operating systems. The implementation method in this community service project consists of three main stages: preparation, execution, and evaluation. Each stage plays a crucial role in achieving the goal of enhancing students' competencies in operating system security.

1. Preparation Stage

The preparation stage is the initial step that is critical to ensuring the smooth execution of the activities. During this stage, several activities are carried out as follows:

a. Initial Information Gathering: The community service team collects data regarding the students' initial understanding of operating system security to assess their knowledge level before training begins.
b. Preparation of Training Materials and Modules: Relevant training materials and modules are developed, tailored to the students' needs, including hardening techniques for Windows and Linux operating systems.
c. Coordination with School Authorities: The team coordinates with SMK Negeri 2 Tegal, located at Jalan Wisanggeni No. 1, Kejambon, Tegal City, Central Java, to ensure the readiness of facilities, such as computer laboratories, and to finalize the schedule for the activities.
d. Pre-Test Data Collection: A pre-test consisting of 20 questions is conducted to measure the students' initial understanding of basic concepts in operating system security, serving as a reference for evaluation at the end of the activities.
e. Training Overview: The main activity involves training using a blended learning approach, which includes both theory and practical sessions. Table 1 and figure 1 below are details of the activities carried out.

Table 1. Activity Schedule Details

Time	Activities	Executive
07.00-08.00	Preparation and attendance of participants	Teachers and laboratory staff of SMK 2 Tegal
08.00-08.15	Opening	PKM Team Leader Achmad Sutanto, S.Kom.,M.Tr.T
08.15-08.30	Welcome from partners	Teacher of SMK 2 Tegal Siswoyo, S.Kom
08.30-08.50	Pre-test	Students of class XI TKJT-2
08.50-10.30	Material presentation-1	Lecturers and students
10.30-10.45	Rest	PKM Team Leader
10.45-11.45	Material presentation-2	Lecturers and students
11.45-12.05	Post-test	Students of class XI TKJT-2
12.05-12.20	Presentation of prizes to the most active participants and highest test scores	All participants
12.20-12.30	Closure	The entire PKM team

2. Execution Stage

The execution stage is the core of the community service activities, where students receive direct training. The participants of the training are 33 students from the eleventh grade of the Computer Network Engineering and Telecommunications (TKTJ) program at SMK Negeri 2 Tegal. The activities in this stage include:

a. Opening Ceremony: The activities begin with a welcome address from school authorities and the community service team, explaining the objectives and benefits of the training.
b. Theory Session: The material on operating system security and hardening techniques is presented interactively. Students are encouraged to engage in discussions and ask questions to deepen their understanding.
c. Practical Session: Following the theory session, students participate in hands-on practice in the computer laboratory. They apply the hardening techniques that have been taught, with guidance from the community service team.
d. Monitoring During Activities: The community service team monitors the students to ensure they can follow the training effectively. Observations are made to assess student engagement and understanding during the practical sessions.

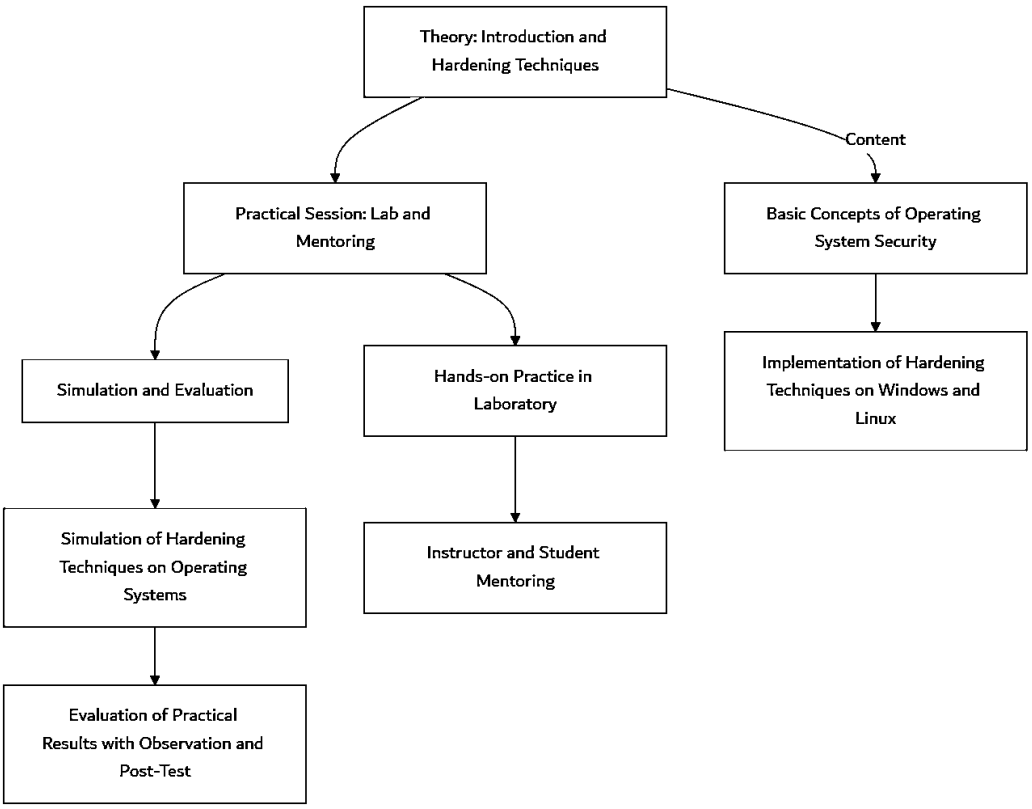

Figure 1. Flowchart of OS Hardening Training Program

3. Evaluation Stage

The evaluation stage aims to measure the effectiveness of the training conducted. The activities in this stage include:

a. Post-Test Implementation: After the practical session, a post-test consisting of 20 questions is conducted to assess improvements in students' understanding and skills. The results are compared with pre-test results to evaluate progress.
b. Simulation of Hardening Techniques Application: Students participate in simulations to test their understanding of the hardening techniques learned, ensuring they can implement the knowledge in real-world situations.
c. Analysis of Evaluation Results: The evaluation results are analyzed to determine the training's effectiveness. A significant increase in the average post-test score indicates the program's success in enhancing students' competencies.

Monitoring was conducted during the activity to ensure that students could follow the training well. At this stage, lecturers and students made direct observations during laboratory practice to assess the application of hardening techniques. Evaluation was also carried out using a post-test to measure the improvement in students' skills in securing Windows and Linux-based operating systems.

C. RESULTS AND DISCUSSION

1. Activity Steps

a. Operating System Hardening Material Presentation

In the first phase of the activity, material was delivered which combined counselling on the importance of operating system security and hardening techniques on Windows and Linux. This activity aims to provide a basic understanding of cyber threats and how hardening techniques can be used to reduce the potential for attacks on operating systems. The delivery of the material was done in an interactive manner, where participants were encouraged to ask questions and discuss them. Figure 2 shows the lecturer explaining the material about operating system hardening, followed by participants who were very enthusiastic about participating in this session. In the picture, the participants focus on listening to the material provided and actively discussing and asking questions about the application of the security measures described.

Figure 2. Delivery of Operating System Hardening Material

b. Hands-on Practicum in the Laboratory
In addition to theory, this training also included a practicum in which participants were given the opportunity to apply the hardening techniques that had been taught. The practicum was conducted with the direct assistance of lecturers and students, who acted as facilitators. During this session, students were taught how to restrict user access, disable unnecessary services, and instal security updates on Windows and Linux operating systems.

Figure 3. Participants practice operating system hardening accompanied by lecturers and students

The documentation in Figure 3 shows students working in the laboratory applying the hardening steps using their own computers. Mentoring ensures that students understand each stage of the practice.

c. Simulation and Evaluation
After the practicum session, a simulation was conducted to test the students' understanding of the application of hardening techniques. Students were asked to simulate security on the operating system and show the results of applying these steps. Evaluation was done through direct observation, as well as pre-test and post-test, to measure the improvement of students' understanding and skills in applying the techniques that have been learned.

2. Monitoring and Evaluation

During the training activities, monitoring was conducted by providing a pre-test before the activities began and a post-test after completion. This test aimed to measure changes in students' understanding of the basic concepts of operating system security, with details of the material as follows:

a. Basic concepts of operating system hardening.
b. Security configuration in Windows and Linux.
c. Restriction of user access and removal of unnecessary services.
d. Firewall and network policy settings.
e. Application of security patches and updates.

Participants' test scores are shown in Table 2.

Table 2. Participants' Pre-Test and Post Test Scores

No.	Participant's Name	Score		Description
		Pre-Test	Post-Test	
1	Ahmad Nur Aji	100 / 100	95 / 100	Score decreased
2	Ainnah Lysyah	90 / 100	100 / 100	Score increased
3	Alfira Hanisah	70 / 100	100 / 100	Score increased
4	Aliefya Mahalva Ardiandra	30 / 100	50 / 100	Score increased
5	Andika Rafi P	40 / 100	80 / 100	Score increased
6	Astin Oktaviani Putri	65 / 100	100 / 100	Score increased
7	Asty Aulia Agustine	50 / 100	20 / 100	Score decreased
8	Aulia Khalda Dzakira	90 / 100	100 / 100	Score increased
9	Ayyu Naili Farah	60 / 100	85 / 100	Score increased
10	Azka Afrilias Zaki	80 / 100	100 / 100	Score increased
11	Bunga Cahya P	90 / 100	100 / 100	Score increased
12	Dava Bintanggg Mp	70 / 100	80 / 100	Score increased
13	Fajar Ragil Saputra	55 / 100	25 / 100	Score decreased
14	Farel Destian Fargas	95 / 100	100 / 100	Score increased
15	Indah Muhafidzoh	40 / 100	25 / 100	Score decreased
16	Islahkul Ardhi	30 / 100	20 / 100	Score decreased
17	Jihan Rahmawati	100 / 100	100 / 100	Best score
18	Laura Ramadhani	85 / 100	80 / 100	Score decreased
19	M Faozan Faqih	65 / 100	55 / 100	Score decreased
20	M Yuda Pratama	100 / 100	90 / 100	Score decreased
21	M. Aditya Pratama	35 / 100	20 / 100	Score decreased
22	Meilisah Dwi Ananda	40 / 100	95 / 100	Score increased
23	Muhammad Asy'kar	90 / 100	100 / 100	Score increased
24	Nadia Yuliana	65 / 100	100 / 100	Score increased
25	Nadin Farisca Imaniar	0 / 100	55 / 100	Score increased
26	Nathanael Juan Riquel Kusumo	70 / 100	85 / 100	Score increased
27	Nurul Amalia	100 / 100	100 / 100	Best score
28	Rahma Citra Dwi Azzahra	100 / 100	100 / 100	Best score
29	Reihanaya Nikeisha Hakim	0 / 100	100 / 100	Score increased
30	Rizal Fadli A	40 / 100	100 / 100	Score increased
31	Salsa Nurul Aeni	50 / 100	95 / 100	Score increased
32	Siti Meilani Khoiriyah	90 / 100	100 / 100	Score increased
33	Tegar Setiawan	70 / 100	100 / 100	Score increased
	Average	66	81	

The test results showed a significant increase in the students' understanding. The average student pre-test score was 66, while the average post-test score increased to 81, an increase of 22.7%. This indicates that the training activity succeeded in improving the students' understanding and skills in applying hardening techniques to the operating system.

3. Effect of Activities on Objectives

Compared with previous studies, this activity showed results consistent with existing findings in the literature regarding blended-learning-based training and the application of hardening techniques. A study by Soares et al. (2023) showed that training that combines theory and hands-on practice can significantly improve student understanding (Soares et al., 2023), which was also found in this work. Another study by Riggs et al. (2023) states that operating system hardening training, especially on Windows and Linux, can significantly reduce the risk of cyber threats (Riggs et al., 2023), which is in line with the results achieved in this activity, where students successfully implemented security measures on their operating systems. In addition, the positive impact of this activity can be seen in the improvement of students' technical skills, as measured through practical tests and evaluations. This is in line with research by Siwakoti et al. (2023) which shows that learning approaches that prioritise the development of practical skills through hands-on exercises can improve students' competence in managing and securing information systems (Siwakoti et al., 2023).

4. Contributions and Implications

This activity made a significant contribution to strengthening cyber security literacy among students of SMK Negeri 2 Tegal, especially those in the Computer Network and Telecommunications Engineering Department. The success of this service shows the importance of practice-based training in improving student competence in operating system security, which will be very useful in facing the demands of the world of work in industries that increasingly require qualified technical skills in this field. The implications of this activity also include the importance of integrating operating system security materials into the vocational school curriculum. By strengthening the practical skills acquired by students, schools can better prepare them to face challenges in the professional world.

5. Obstacles Faced and Solutions

Although this training activity had a positive impact, there were some obstacles encountered, one of which was the limited time that prevented students from fully practising hardening techniques. This made not all students able to master the steps taught optimally, especially in applying the techniques to more complex operating systems, such as Linux. To overcome this problem, it is recommended to extend the duration of training and

provide more time for practicum sessions in the future. Additional sessions should be conducted to provide technical assistance to students who experience difficulties. It is also necessary to develop training materials to cover more complex security techniques that are relevant to the needs of the industrial world so that students can further deepen their skills in securing operating systems.

D. CONCLUSIONS AND SUGGESTIONS

The implementation of operating system security training through hardening techniques at SMK Negeri 2 Tegal successfully achieved predetermined objectives, namely improving students' skills in securing Windows and Linux operating systems. Through a blended learning approach that combines theory and hands-on practice, participants can understand and effectively apply hardening techniques. The results of the activity implementation showed a significant increase in students' understanding of operating system security, with the average post-test score increasing by 22.7%, from 66 to 81. This reflects the strengthening of students' soft and hard skills when facing cybersecurity challenges in the world of work.

Although the results achieved were satisfactory, some challenges and obstacles still arose, such as limited time in completing the material and some students needing more intensive assistance in practice. Therefore, it is recommended that this training activity be continued with further training to strengthen students' understanding and skills, as well as to adjust the material to the development of increasingly complex cyber threats. In addition, the integration of operating system security materials into the regular SMK curriculum is expected to strengthen students' readiness to face the industrial world. Further research or services that can develop more in-depth and structured training modules, as well as applications in other fields such as network security or software development, are also highly recommended.

ACKNOWLEDGMENTS

We thank the Institute for Community Service of Politeknik Harapan Bersama (P3M) for providing funding support for the implementation of this activity through Funding Decree No. 211.05/PHB/XII/2024. We also thank SMK Negeri 2 Tegal, especially the Computer Network and Telecommunication Engineering Study Program, which provided facilities and actively participated in the smooth running of the activity. We also appreciate the participation of students who were involved as facilitators as well as students who enthusiastically participated in the training. Contributions from all parties are valuable for the successful implementation of this service.

REFERENCES

Affia, A. O., Nolte, A., & Matulevičius, R. (2023). IoT Security Risk Management: A Framework and Teaching Approach. *Informatics in Education*, *22*(4), 555–588.

Allison, J. (2023). Devising a cyber security management module through integrated course design. *Journal of Further and Higher Education*, *47*(10), 1389–1403.

Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(1), 71. https://doi.org/10.1057/s41599-023-01560-x

Jerman Blažič, B., & Jerman Blažič, A. (2022). Cybersecurity skills among European high-school students: A new approach in the design of sustainable educational development in cybersecurity. *Sustainability*, *14*(8), 4763.

Kursuncu, U., Yang, K.-C., Pierri, F., Deverna, M. R., Mejova, Y., & Blackburn, J. (2023). CySoc 2023: 4th International Workshop on Cyber Social Threats. *Companion Proceedings of the ACM Web Conference 2023*, 1307–1307. https://doi.org/10.1145/3543873.3589747

Laundon, M., McDonald, P., & Greentree, J. (2023). How education and training systems can support a digitally-enabled workforce for the manufacturing industry of the future: an exploratory study. *Education+ Training*, *65*(6/7), 909–922.

McIntosh, T., Susnjak, T., Liu, T., Xu, D., Watters, P., Liu, D., Hao, Y., Ng, A., & Halgamuge, M. (2024). Ransomware Reloaded: Re-examining Its Trend, Research and Mitigation in the Era of Data Exfiltration. *ACM Computing Surveys*, *57*(1), 1–40. https://doi.org/10.1145/3691340

Onyango, E., & Kelonye, C. (2022, September). Artificial Intelligence (AI) Driven Interventions in Technical and Vocational Education and Training. *Tenth Pan-Commonwealth Forum on Open Learning*. https://doi.org/10.56059/pcf10.1996

Oruc, A., Chowdhury, N., & Gkioulos, V. (2024). A modular cyber security training programme for the maritime domain. *International Journal of Information Security*, *23*(2), 1477–1512.

Radoglou-Grammatikis, P., Kioseoglou, E., Asimopoulos, D., Siavvas, M., Nanos, I., Lagkas, T., Argyriou, V., Psannis, K. E., Goudos, S., & Sarigiannidis, P. (2023). Surveying Cyber Threat Intelligence and Collaboration: A Concise Analysis of Current Landscape and Trends. *2023 IEEE International Conference on Cloud Computing Technology and Science (CloudCom)*, 309–314. https://doi.org/10.1109/CloudCom59040.2023.00057

Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., Vuda, K. V., & Sarwat, A. I. (2023). Impact, Vulnerabilities, and Mitigation Strategies for Cyber-Secure Critical Infrastructure. *Sensors*, *23*(8), 4060. https://doi.org/10.3390/s23084060

Safitra, M. F., Lubis, M., & Fakhrurroja, H. (2023). Counterattacking Cyber Threats: A Framework for the Future of Cybersecurity. *Sustainability*, *15*(18), 13369. https://doi.org/10.3390/su151813369

Siwakoti, Y. R., Bhurtel, M., Rawat, D. B., Oest, A., & Johnson, R. C. (2023). Advances in IoT Security: Vulnerabilities, Enabled Criminal Services, Attacks, and Countermeasures. *IEEE Internet of Things Journal*, *10*(13), 11224–11239. https://doi.org/10.1109/JIOT.2023.3252594

Soares, R. V., Barel, P. S., Leite, C. C., Letícia dos Santos, L., Junior, F. C. S., de Carvalho, E. R., Gianotto-Oliveira, R., & Cecilio-Fernandes, D. (2023). Implementation of Escape Room as an Educational Strategy to Strengthen the Practice of Safe Surgery. *Journal of Surgical Education*, *80*(7), 907–911. https://doi.org/10.1016/j.jsurg.2023.04.016

Sutanto, A. (2024). *Sistem Operasi Berbasis Linux: Panduan Lengkap bagi Pemula untuk Menguasai Linux dan Dasar Konfigurasi Jaringan* (1st ed.). CV Bravo Press Indonesia.

Wiratama, A. D. (2023). Cyber Security In 2023: The Latest Challenges And Solutions. *Jurnal Komputer Indonesia*, *2*(1), 47–54. https://doi.org/10.37676/jki.v2i1.569