
Baseline Training for Digital Infrastructure Protection

Muhammad Akram Hamzah^{1*}, Ruhamah², Siaulhak³ and Safwan Kasma⁴

^{1,2,3,4}Department of Informatics, Universitas Cokroaminoto Palopo, Palopo, Indonesia.

*E-mail: akramhamzah@gmail.com

Abstract

The increasing reliance on digital technology has led to increased vulnerabilities in network infrastructure, thus requiring a strong understanding of network security among college students. The objective of this community service program was to improve students' knowledge of network security principles. The program involved 38 students and included a combination of theoretical instruction and practical exercises, utilizing the WHATSMYIP application to trace IP addresses. The results showed that 85% of participants demonstrated an improved understanding of network security concepts, with feedback reflecting an increased awareness of digital threats. The training not only equipped the students with essential skills to manage and protect digital infrastructure but also encouraged a proactive approach to addressing information security challenges. Furthermore, the program emphasized the importance of securing digital environments in educational settings, highlighting the role of students as future guardians of information technology. This initiative contributes to the development of digital competencies among students, preparing them for future careers in a technology-driven world and supporting local innovation.

Keywords: Digital Infrastructure, Network Security Testing, Whatsmyip.

Introduction

Network Security is a set of policies, processes, and practices designed to protect computer networks, data, and resources from unauthorized access, misuse, damage, or attack (Dastres & Soori, 2021; Pratama et al., 2024). Network security aims to maintain the confidentiality, integrity, and availability of information on the network (Amin et al., 2022; Bustami & Bahri, 2020; Fairuzabadi et al., 2023).

A computer network is a system that allows two or more devices to communicate with each other and exchange data or information (Tangkowit et al., 2021). In this case, network security testing is very important to maintain the protection of existing digital infrastructure (Prasetyo et al., 2024). Digital infrastructure, which includes computer networks and connected systems, requires proper security to avoid threats that can damage or steal valuable data (Laksana & Mulyani, 2024). Network security testing aims to identify potential

Received: 02 March 2025

Revised: 24 April 2025

Accepted: 27 April 2025

Available Online: 28 May 2025



security gaps in the network that can be exploited by irresponsible parties (Alanda et al., 2020; Azmi, 2023)

At SMAN 15 Luwu, although internet network facilities are available, inadequate connection quality poses a challenge in maintaining smooth communication and security of transmitted data. For this reason, the protection of digital infrastructure in this school is very important, especially in ensuring that the network used remains safe from potential cyber threats.

Seeing these conditions, community service is the right means to mediate the campus and students at SMAN 15 Luwu in overcoming existing problems. Cokroaminoto University Palopo (UNCP) lecturers play a role in conducting community service by providing a basic understanding of network security and network security testing that can be done to protect digital infrastructure. One of the applications introduced in this activity is Whatsmyip, which is used to check the network status and ensure that the IP address used in the network system is secure (Kolonias & Forsberg, 2020). This application can help students understand more about the importance of network security testing and data protection in the context of using computer networks in schools.

Through this service, it is hoped that students of SMAN 15 Luwu can gain better knowledge about network security testing and how to protect their digital infrastructure from potential threats. This activity also aims to improve their skills in maintaining the security of data and information within the school network.

Materials and methods

The training was conducted using a structured and participatory approach to ensure that participants not only understood the concepts taught, but were also able to apply them in a real-life context. The implementation method consists of several stages as follows:

A. Activity Schedule

This activity was carried out by the Informatics Service team, Faculty of Computer Engineering, Cokroaminoto University Palopo on January 13, 2025 at SMAN 15 Luwu which is located on the Palopo-Makassar Axis Road No.KM.28, Tirowali, Kec. Ponrang, Luwu Regency.

B. Activity Implementation

The implementation methods used in this training program or activity are:

1. Preparation Stage

This preparation stage has been passed by the service team to obtain the necessary data and as material for compiling the service proposal..

The steps taken in this preparation stage are:

- a. Observation of the training target sit
- b. Determination of problems faced by students in SMAN 15 Luwu
- c. Obtain venue permit

2. Implementation Stage

The method used in the implementation of this service activity is a combination of counseling lectures and training practices using computer devices. This training will be carried out using tools such as laptops, sound systems, and LCD projectors.

3. Final Stage

Preparation of the final report of the training program.

C. Reporting and Documentation

During the training, all activities were documented in the form of photos, videos, and daily notes. This documentation is used to make the final report and also as publication material for community service activities.

The service team then compiled a complete report covering all stages of training implementation, results, and evaluation. This report is submitted to the school and related agencies as proof of implementation and to be used as a reference for similar activities in the future.

Results

This training was held for one day, on January 13, 2025, with a method that combines theory and practice. The material presented included a basic understanding of network security testing, ways to protect digital infrastructure, and the use of the Whatsmyip application to check network security status. The results of the implementation showed that the participants' enthusiasm for explanations, demonstrations, and assistance was very high. Here are some documentation of the training conducted:



Figure 1. Opening Ceremony



Figure 2. Material Provision

Participants actively followed instructions, although some had difficulty in following some of the steps explained.

The success of this activity was also supported by good coordination with the school, the high enthusiasm of the participants in improving their skills, the materials that were appropriate to the needs, and the ability of the participants to follow the demonstration appropriately.

Discussion

From the results that have been carried out, it appears that the needs of participants in terms of increasing knowledge about network security testing and digital infrastructure protection are needed in the environment of SMAN 15 Luwu. This finding became the basis for choosing the right training theme, namely network security testing: basic understanding for digital infrastructure protection at SMA Negeri 5 Luwu.

The implementation of the training by combining theoretical and practical methods proved effective in delivering the material comprehensively. Although there were some obstacles, especially in following the practical steps, the enthusiasm and active participation of the participants showed that the approach used was appropriate. This indicates that the participants did not only passively receive information, but also tried to implement what they had learned.

Supporting factors for the success of the training, such as good coordination between the organizers and SMAN 15 Luwu, as well as materials tailored to the needs of the participants, contributed to the smooth running of the activity. Thus, this training is expected to not only improve students' technical skills in network security, but also prepare them to face the challenges of a working world that is increasingly dependent on digital security technologies and systems.

Conclusion

The network security testing training at SMA Negeri 15 Luwu showed that improving students' knowledge and skills in maintaining digital infrastructure is really needed. Through a theoretical and practical approach, participants not only gained a basic understanding, but were also able to try out the application directly, even though they still faced technical obstacles. The enthusiasm and active participation of students prove that this activity is relevant to their needs. With good coordination and materials tailored to the school's conditions, this training has succeeded in making a real contribution to preparing students to face technological developments and cyber threats in the future.

Acknowledgement

The authors would like to express their deepest gratitude to SMAN 15 Luwu, especially to the principal, teachers, and all staff who have given permission, support, and facilities in the implementation of this service activity. We greatly appreciate the warm welcome and active participation of the teachers in accompanying the students during the training. The author is also grateful to the students who have participated in this activity with enthusiasm. Their enthusiasm and curiosity in understanding the concept of network security testing is a great motivation for us in sharing knowledge.

References

- Alanda, A., Satria, D., Mooduto, H. A., & Kurniawan, B. (2020). Mobile Application Security Penetration Testing Based on OWASP. *IOP Conference Series: Materials Science and Engineering*, 846(1). <https://doi.org/10.1088/1757-899X/846/1/012036>
- Amin, M., Raja, H. D. L., Nur, M. N. A., Prasetio, A., Sulaiman, O. K., Karim, A., Muttaqin, Sihotang, J. I., Simarmata, J., Jamaludin, Harlina, S., A. A., & Pakpahan, A. F. (2022). *Teknologi Jaringan Nirkabel*. Yayasan Kita Menulis.
- Azmi, Z. A. I. (2023). Implementation of a Network Security System Using the Port Knocking Method at Taruna Satria Vocational School Pekanbaru. *Jurnal Inovtek Polbeng*, 9(2). <https://doi.org/10.35314/f5pjjj80>
- Bustami, A., & Bahri, S. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi : Systematic Review. *Unistek*, 7(2), 59–70. <https://doi.org/10.33592/unistek.v7i2.645>
- Dastres, R., & Soori, M. (2021). A Review in Recent Development of Network Threats and Security Measures Computer Integrated Manufacturing View project Modern CAD/CAM Systems View project. *Article in International Journal of Computer and Information Sciences*.
- Fairuzabadi, M., Pangaribuan, J. J., Moedjahedy, J. H., Sihotang, J. I., Simarmata, J., A. A., Jaya, A. K., Sasongko, D., Turnip, T. N., Suardinata, Yasir, F. N., Gustiana, Z., Rizal, M., & Pungus, S. R. (2023). *Keamanan Sistem Informasi dan Kriptografi*. Yayasan Kita Menulis.
- Kolonia, A., & Forsberg, R. (2020). *Preserving Security and Privacy: a WiFi Analyzer Application based on Authentication and Tor*. 2020:546, 79.
- Laksana, T. G., & Mulyani, S. (2024). Pengetahuan Dasar Identifikasi Dini Deteksi Serangan Kejahatan Siber Untuk Mencegah Pembobolan Data Perusahaan. *Jurnal Ilmiah Multidisiplin*, 3(01), 109–122. <https://doi.org/10.56127/jukim.v3i01.1143>
- Prasetyo, S. E., Kaharuddin, W., Informasi, T., Komputer, F. I., & Batam, U. I. (2024). *Optimalisasi Keamanan Jaringan Di Era Digital menggunakan Metode Zero Trust*. 05(03), 15–24. <https://doi.org/10.37253/joint.v5i3.9986>
- Pratama, A. M., Syaiful, & Rahman, M. F. (2024). *Keamanan Data dan Informas*. Kaizen Media Publishing.
- Tangkowit, A. E., Palilingan, V. R., & Liando, O. E. S. (2021). Analisis Dan Perancangan Jaringan Komputer Di Sekolah Menengah Pertama. *Edutik : Jurnal Pendidikan Teknologi Informasi Dan Komunikasi*, 1(1), 69–82. <https://doi.org/10.53682/edutik.v1i1.1044>