TEPIAN Vol. 4 No. 4 (December 2023) p-ISSN 2721-5350 e-ISSN 2721-5369
doi.org/10.51967/tepian.v4i4.2910

Wireless Computer Network (WLAN) Security Test at Pradita University

Banu Bagaskara
Informatics, Pradita University, Banten, 15810, Indonesia
banu.bagaskara@student.pradita.ac.id

Handri Santoso *
Informatics, Pradita University, Banten, 15810, Indonesia
handri.santoso@pradita.ac.id
**Corresponding Author*

Submitted: 2023-07-24; Accepted: 2023-11-01; Published: 2023-12-31

***Abstract*—**In this day and age, information technology has developed rapidly, one of which is wireless computer network technology called Wireless Local Area Network (WLAN). Agencies and individuals have widely used the use of wireless computer networks. Because with a wireless computer network, it is easy to connect the devices so that your work becomes quickly completed. Along with the development of wireless computer networks, problems will undoubtedly arise, one of which is about network security in wireless technology; therefore, to maintain network stability, it is necessary to conduct periodic evaluations. To analyze network security with the Penetration Testing method simulated attacks on the network, the operating system with the correct specifications is Kali Linux. Kali Linux is designed for network security testing, equipped with tools that support hacking activities, and as a tool to test network security. The results of this research can later be used to improve the security of wireless computer networks at Pradita University. This study concludes that during the design of WLAN Network Security Analysis using attacks (Cracking The Encryption, Denial of Service, and MITM) using Kali Linux at Pradita University, it can be concluded that the security owned by the Pradita University WLAN network still has many loopholes to exploit**.**

***Keywords*—**Wireless Network, Network Security, Wireless LAN

I. INTRODUCTION

In today's era, technology is advancing very quickly in all aspects of life, including information technology; the development of information and communication technology is necessary (Saskara, Gede Arna Jude and Indrawan, I Putu Oktap and Putra, 2019). Because knowledge and communication technology are difficult to separate from people's lives in a fast-moving era like today. Wireless Local Area Networks (WLAN) or wireless local network technology is one of the information and communication technology advances (Setiadi, Ibnu Hanafi and Afrianto, 2019). Wireless technology is often found in restaurants, offices, campuses, and public places, but only some pay attention to data communication security on *wireless* networks. As a result, *hackers* are curious to try their ability to carry out illegal activities using existing wireless networks (Xing, 2023). In terms of safety, wireless networks are more vulnerable than networks that use cables. One reason is that it is easy for general users to connect to WLAN networks, so security issues must be considered. Wireless networks use radio waves as a transmission medium, making the network more vulnerable to intruders (Trungadi, 2023).

As essential as it is to create an efficient system, network, or application, it is even more crucial to protect and provide a secure service. This has never been more true than in today's society: as technology advances, so too do risks and security concerns. Cybersecurity and cybercrime are inversely correlated concepts that go hand in hand (Masyhur, Zulkarnaim and Hartono, 2023). Cyber security protects hardware, software, and data related to the internet from various threats, whereas cybercrime is the unlawful activity that uses a computer as its primary means of commission and theft. The inverse correlation between the two demonstrates their relationship; if cybersecurity measures are enhanced and expanded, the likelihood of cybercrime is diminished. However, if cybersecurity is inadequate, the likelihood of cybercrime increases significantly (Widerberg Palmfeldt, Alva and Mattsson, 2023).

Computer networks have experienced very rapid development. Along with the increasing needs of computer users connected to a computer network, infrastructure is also needed to accommodate users' requests and empower available resources. STMIK Mataram has made many uses of computer network technology. The use of network technology is carried out to support lecture activities and activities related to administration. Therefore, all information sent through a computer network needs attention (Samsumar, Lalu Delsi and Gunawan, 2017).

Wireless networks are currently in the spotlight regarding the level of security, so it needs serious attention because they utilize radio waves emitted by broadcast and move freely in the air so that anyone can capture them anytime (Catalano, Christian and Pagano, Alessandro and Piccinno, Antonio and Stamerra, 2023). The design and implementation of a network topology, in this case, a wireless computer network, cannot be relied upon casually; a further process is needed to penetrate the network's capabilities to remain in accordance with the design purpose (Turban, Efraim and King, David and

Banu , B., & Santoso , H. (2023). Wireless Computer Network (WLAN) Security Test at Pradita University. TEPIAN, 4(4). https://doi.org/10.51967/tepian.v4i4.2910

Lee, Jae Kyu and Liang, Ting-Peng and Turban, Deborrah C and Turban, Efraim and King, David and Lee, Jae Kyu and Liang, Ting-Peng and Turban, 2015). Therefore, an assessment of the availability, confidentiality, and integrity of a computer network is needed so that the performance of the computer network is reliable. By conducting regular and periodic evaluations of existing computer networks, because of the dynamic development of technology so that vulnerabilities continue to grow as well, so it is hoped that holes or security holes that exist in the wireless computer network system that is running so that a good and reliable wireless computer network security system model can be made (Demertzi, Vasiliki and Demertzis, Stavros and Demertzis, 2023).

This evaluation is carried out to increase awareness of the management of security problems or *intrusion detection* and how quickly the ability to respond to threats (Staddon, Edward and Loscri, Valeria and Mitton, 2023).

In general, there are two categories of vulnerabilities in wireless networks: configuration flaws and inadequate encryption. Because it is now so simple to create a wireless network, the following are examples of the causes of structural defects (Boodai, Jawhara and Alqahtani, Aminah and Frikha, 2023). Some vendors provide facilities that make it simpler for users to find wireless networks that still use the vendor's default wireless configuration. The wireless network administration process frequently utilizes the vendor's default settings, such as IP Address, remote management, SSID, and DHCP, without encryption of the user and password (Zen, Bita Parga and Saputra, 2023).

In order to evaluate the efficacy of network security, the network's security system must be evaluated. Penetration Testing is a technique for assessing network security that involves replicating web-based attacks (Syaputera, Angga and Riska, Riska and Mardiana, 2023).

To analyse network security with the Penetration Testing method simulated attacks on the network, the operating system with the correct specifications is Kali Linux. Kali Linux is designed for network security testing, equipped with *tools* that support hacking activities, and as a tool to test network security (Turban, Efraim and King, David and Lee, Jae Kyu and Liang, Ting-Peng and Turban, Deborrah C and Turban, Efraim and King, David and Lee, Jae Kyu and Liang, Ting-Peng and Turban, 2015).

Pradita University is a campus that uses WLAN technology for various purposes; students, lecturers, or employees do not infrequently use wireless networks for academic or non-academic purposes (Lutfiani, Ninda and Wijono, Sutarto and Rahardja, Untung and Iriani, Ade and Aini, Qurotul and Septian, 2023). Therefore, the frequent use of wireless networks does not rule out the possibility of abuse by irresponsible people, so prevention is needed by knowing the level of wireless network security so that hacking does not cause losses.

II. LITERATURE REVIEW

A. Computer Network

A computer network is a system that connects two or more computers. Now the development of computer networks is becoming increasingly rapid; previously used cables to connect one computer to another computer now use technology without wires, which can be called *wireless*. Many agencies have used this technology and competed with each other to develop it so that many users can easily access it. Therefore the infrastructure that can accommodate requests from users and storage of the system must be improved due to the increasing needs of the system (Murumba Julius, Mukisa and Muhambe Titus, 2023).

Wireless (wireless) is a technology that can connect two *devices* in the form of computers, laptops, or mobile phones without using cables to exchange data or information. One of the standard devices used to communicate in wireless local networks (*Wireless Local Area Network* / WLAN) is *Wireless Fidelity* (WiFi) based on the IEEE 802.11 specification. It is a commonly used standard in international wireless communications(Saskara, Gede Arna Jude and Indrawan, I Putu Oktap and Putra, 2019).

B. WLAN (Wireless Local Area Network)

Wireless Local Area Network is a communication system with a small coverage or a flexible Local Area Network the sender and receiver of data through air media using radio frequency technology (Agustio, Dino Pandu and Nainggolan, 2023). So that the device can move quickly because it is not tied to a cable (Ojha, Nitish Kumar and Baray, 2023). WLAN can be divided into two main categories, namely:

1. *Wireless* LAN *Ad-Hoc mode*

Ad-hoc mode network model, the network between one device and another device is carried out spontaneously / directly without going through specific configurations as long as the transmitter's signal can be appropriately received by the receiving apparatus, namely the receiver (Setiadi, Ibnu Hanafi and Afrianto, 2019).

2. *Wireless* LAN Infrastructure mode

The infrastructure mode network model provides a connection between devices connected to a WLAN network; an intermediary *device* is needed as *an access point* connected to a wired computer network before transmitting to signal-receiving devices (Haq, Inam Ul., Ramzan, Saba., Ahmad, Nazir., Ahmad, Yasir., and Nadeem, 2023).

The vulnerability of wireless networks (*Wireless* LAN) to the security of data, information, and service availability is a topic of concern and discussion among practitioners (Saskara, Gede Arna Jude and Indrawan, I Putu Oktap and Putra, 2019). For this reason, it is stated in a theory that a computer network is said to be safe and reliable if it meets the elements:

Banu , B., & Santoso , H. (2023). Wireless Computer Network (WLAN) Security Test at Pradita University. TEPIAN, 4(4). https://doi.org/10.51967/tepian.v4i4.2910

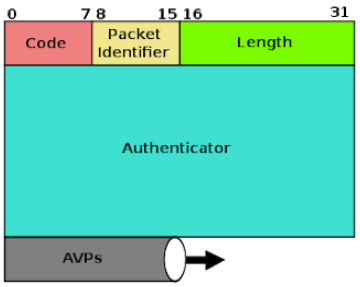
1. *Privacy* and *Confidentiality*: A mechanism that is carried out to protect information from network users who do not have rights, while *confidentiality* is more directed to the purpose of the information provided and should only be for that purpose.
2. *Integrity*: Aspects prioritise access to information intended for specific, the integrity of the data is still maintained.
3. *Authentication*: This section prioritises the validity of users who access data, information, or services from an institution.
4. *Availability*: Aspects related to the availability of data, information, or services when such data, information, or services are required.
5. *Access Control*: This aspect relates to the classification of users and the way users access information.
6. *Non-Repudiation*: Aspects related to user recording, which aims to avoid denial of users who have penetrated services, data, and available information(Saskara, Gede Arna Jude and Indrawan, I Putu Oktap and Putra, 2019).

Along with the times, *wireless* LAN networks began with many agencies or individuals. This requires the importance of security because of the many attack loopholes on wireless networks. Attacks that most often appear on *this* wireless network as several attacks that generally appear on wireless networks are as follows:

1. *Reveal SSID:* An attempted attack exposing the SSID of an *access point* that a computer network administrator intentionally hides.
2. *MAC Address Spoofing: A hacker attempts* to penetrate the security of MAC address filtering by *spoofing* the MAC address on a computer network, using a legitimate user's MAC address to obtain computer network services.
3. *Authentication Attack*: An attack on a legitimate authentication user, causing paralysis or disconnection of the legitimate user. Attackers take advantage of these attacks to gain deeper resources using network services.
4. *Eavesdropping*: An attack using encryption to listen to all packets transmitted by users in an unencrypted computer network.
5. *Session Hijacking*: An attack that attacks a user's session to be used to gain access rights to a service being accessed by an authorised user.
6. *Man In The Middle Attack*: An attack carried out by spoofing a legitimate user so that the target's transmission is to the attacker so that the attacker gets all the information transmitted by the target.
7. *Denial of Service*: An attack that attacks resource availability, causing legitimate users to experience a disconnected connection from a computer network.
8. *Rogue Access Point*: An attack that uses an access point device made the same as an access point located in an institution. So when a legitimate user accesses the access point.(Samsumar et al., 2017)

C. RADIUS (*Remote Authentication Dial-In User Service*)

RADIUS is a computer security protocol used to authenticate, authorise and register user accounts centrally to access a network. An authentication Server is a security device on a computer network that implements an authentication process to serve authentication requests from network service users. This authentication server implements the AAA (authentication, *authorisation, and accounting*) model. *Authentication* attests to the user's (end-user) identity in accessing the network. While accounting is a computational process carried out by a system that records records that wireless computer network users have used. RADIUS has a packet format that is used in transmitting data.(Saskara, Gede Arna Jude and Indrawan, I Putu Oktap and Putra, 2019). Picture 1 show RADIUS Protocol



Picture 1. RADIUS Protocol

1. Code: has a length of one octet (8 bits) and is used to distinguish the type of RADIUS message sent to packets. Here are those codes (in decimal), among others. Table 1 show RADIUS Protocol code

Table 1. Code on the RADIUS Protocol

Code	Description
1	Access – Request
2	Access-Accept
3	Access-Reject
4	Accounting – Request
5	Accounting – Respond
11	Access Challenge
12	Status – Server
13	Status - Client
255	Reserved

2. Packet Identifier: has a length of one octet (8 bits) and aims to match client requests and response packets provided by the RADIUS server.

Banu , B., & Santoso , H. (2023). Wireless Computer Network (WLAN) Security Test at Pradita University. TEPIAN, 4(4). https://doi.org/10.51967/tepian.v4i4.2910

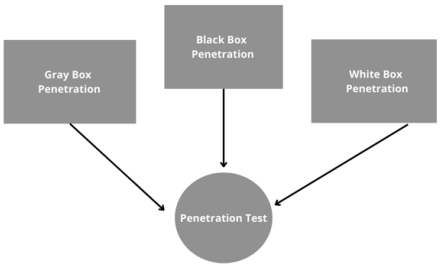
3. Length: has a length of two octets (16 bits) and provides information about the size of the packet, including code, identifier, length, authenticator, and attributes.
4. Authenticator: has a length of 16 octets (128 bits), used to prove replies from the RADIUS server, but also used for password algorithms.
5. Attributes: Attributes contain information that RADIUS messages carry. Each letter can have one or more attributes. Examples of RADIUS attributes: user name, password, CHAP-password, access point (AP) IP address, and reply message. This part of the package contains authentication, authorisation, information, and specific configuration details required for requests from RADIUS clients or NAS.

In practice, the RADIUS server is combined with a captive portal, a traffic routing technique to authenticate and secure data that passes through the internal network to the external network by deflecting user traffic to a login page(Samsumar et al., 2017).

D. Penetration Testing

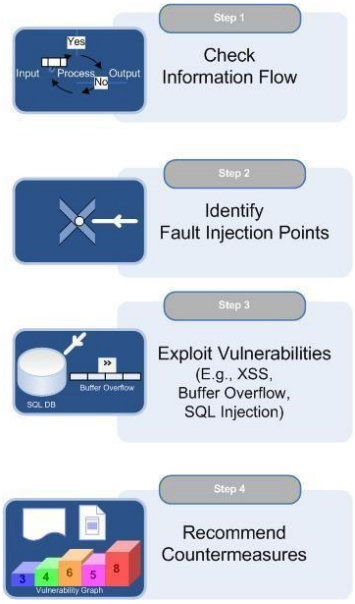
Penetration test, commonly referred to as Pentest, is a method used to evaluate the security of a system and security on a computer network. The evaluation is carried out by conducting a simulated attack (attack). The results of the pentest are significant for administrators as feedback from the system or computer network, which is then improved the level of security of the computer system, besides that input will also be given on the condition of system vulnerability so that it is easier to carry out evaluations of the computer security system that is running. Pentes are also known as "ethical hacking".

Black box, white box, and grey box are examples of available pentesting techniques. Black box testing is the technique of penetration testing that assumes the tester has no knowledge of the infrastructure being tested. Therefore, testers utilizing this approach must attempt to gather all necessary information from the outset, conduct analysis, and determine the type of attack to be executed. In White box testing, the information required to execute a pentest is already known to the tester. Likewise, the grey box incorporates the conditions of the black and white boxes. Full disclosure is an alternative term for the white box, partial disclosure for the grey box, and opaque disclosure for the black box. Picture 2 show Penetration Test method



Picture 2. Penetration Test Method

In general, there are four basic steps taken for pentest activities, namely collecting several important information from the system, conducting analysis to determine the type of attack to be carried out, conducting attack activities to exploit system vulnerability, and conducting reports and recommendations for system improvement(Saskara, Gede Arna Jude and Indrawan, I Putu Oktap and Putra, 2019). Picture 3 show step Penetration Test



Picture 3. Step Penetration *test*

III. METHODS

This test is conducted using actual attacks, natural systems, and accurate data using tools and techniques that hackers often use. In running the test, there are four stages carried out in Penetration Testing: the Planning, Discovery, Attack, and Reporting phases.

Banu , B., & Santoso , H. (2023). Wireless Computer Network (WLAN) Security Test at Pradita University. TEPIAN, 4(4). https://doi.org/10.51967/tepian.v4i4.2910

Picture 4. Pentest Method Stage

A. Penetration Test

A penetration test is carried out to determine holes or security holes contained in the wireless computer network of the Pradita University Penetration test. There are three stages of the type of penetration testing attack that will be tested:

1. Cracking The Encryption
   In the first stage, this attack aims to determine whether all Access Points are protected with encryption security systems such as WEP, WPA, or WPA2.
2. Denial of Service (DoS) Attack
   In the second stage, this attack is carried out to determine whether the network from Pradita University can be turned off, causing legitimate users to experience a disconnected connection from the web.
3. Man In The Middle (MITM) Attack
   In this last stage, the attack aims to intercept data packets from other users connected to the same network.

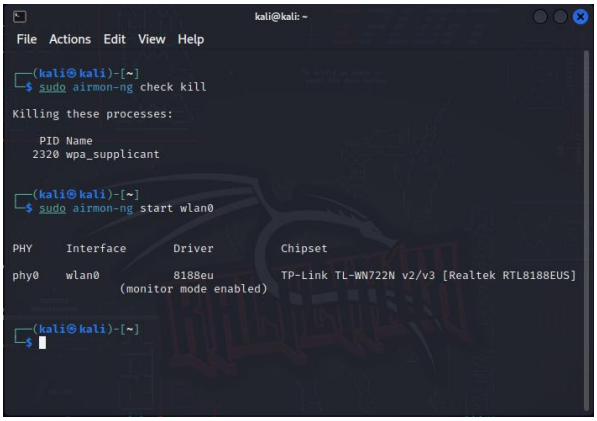
The results of penetration testing get an outcome that can be analysed to determine the vulnerability of the wireless computer network used by Pradita University. Testing was conducted directly on the Pradita University network using attacks that may appear on the wireless computer network in the case study. Episodes for simulated networks include Cracking The Encryption, Denial of Service, and Man In Middle Attacks.

III. Results and Discussion

The implementation stage is implementing the system according to previous needs and designs. In addition, this implementation will also explain how this system will work. The hardware used includes a computer that functions as a place to install Kali Linux. At the same time, the tools used are Aircrack-ng and Ettercap to perform test attacks.

A. Cracking The Encryption

In the first stage, this attack aims to determine whether all Access Points are protected with encryption security systems such as WEP, WPA, or WPA2. The tester scans the Access Point (26:5A:4C:9C: EA:10) and then determines the target for cracking the key used as security shown in Picture 5.



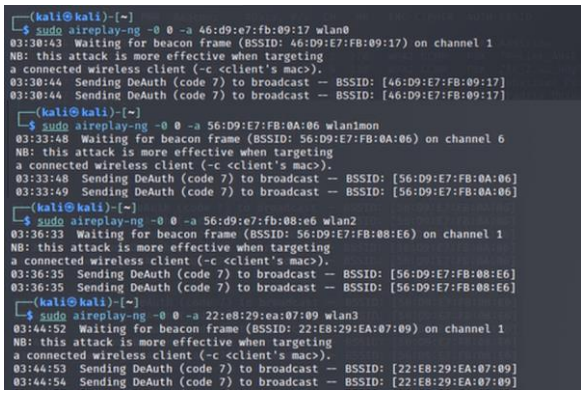
Picture 5. Airmon-ng

From the Cracking the Encryption experiment, it can be concluded that to increase the resistance of passwords to cracking attempts, several things must be done, including:

1. Use WPA, WPA2, WPA-PSK, or WPA2-PSK encryption security types with a security level above WEP.
2. Using a combination of uppercase letters, lowercase letters, numbers, and symbols to create passwords, to complicate attacks with brute-force attacks and dictionaries.
3. Create passwords with more than 15 characters to complicate attacks with brute-force attack methods and dictionaries.

B. Denial of Service (DoS) Attack

This stage is carried out by attacks on wireless services for clients so that it can affect network performance. DoS attack that aims to paralyse the connection of other users on the network. The network at Pradita University uses multiple access points in one network, and the network is challenging to turn off. If it only attacks one access point, it will attack several access points simultaneously. The initial information needed is the password of the tested wireless network so that the tester's computer can connect to the wireless service. Picture 6 shows when performing the DoS Attack stage by attacking 4 Access Points at once



Picture 6. Aireplay-ng send DeAuth

From the results obtained, it can be seen that the length of time the de-authentication attack takes to disconnect the user from the network is influenced by the

Banu , B., & Santoso , H. (2023). Wireless Computer Network (WLAN) Security Test at Pradita University. TEPIAN, 4(4). https://doi.org/10.51967/tepian.v4i4.2910

distance between the tester computer and the user and by the number of targets. The longer the distance between the user and the attacker and the more marks to be attacked, the longer it will take to be hit.

C. Man In The Middle (MITM) attack

In this stage, attacks are carried out on other users of the same WLAN network by intercepting data packets. This test uses the ettercap tool as a test tool. The Ettercap view is shown in Picture 7.

Picture 7. Ettercap Display

At the Man In The Middle Attack stage, the initial condition is that the user and target computers must be connected to the wireless Access Point network "campus". Here the computer tester acts as a third party between the target and the access point that connects the target and the internet service. In this case, the first target of the Ettercap configuration is the gateway of the access point, which is 192.168.124.1, and the second target is the IP of the target computer, which is 192.168.121.35. Picture 8 show the target IP Address.

Picture 8. IP Address of the access point and target computer

The next stage is to perform ARP Poisoning. Address Resolution Protocol (ARP) is a TCP/IP Protocol Suite protocol responsible for resolving IP addresses into Media Access Control (MAC Address) addresses. ARP poisoning is a technique of attacking local computer networks with both wired and wireless media, which 55 allows attackers to find out data frames on the local network, modify traffic, or even stop traffic. In principle, ARP poisoning takes advantage of weaknesses in its computer network technology that uses ARP broadcast.

After that, the sniffing process is run to record the target computer's activities when using internet services. The ettercap results are in Table 2.

Table 2. Ettercap Results

Target 1	Target 2	Information
Access Point (IP: 192.168.124.1)	Target Computer (IP: 192.168.121.35)	http://testphp.vulnweb.com/login.php USER: banban PASS : banban12 http://testphp.vulnweb.com/login.php USER: banban001, PASS : pentest123 http://testphp.vulnweb.com/login.php USER: banbanus PASS : mommy321 http://testphp.vulnweb.com/login.php USER: glenny PASS : tongsong123 http://testphp.vulnweb.com/login.php USER: rikarder PASS : berisik01 http://testphp.vulnweb.com/login.php USER: yuukira, PASS : putih5512 http://testphp.vulnweb.com/login.php USER: darkheaven PASS : asurablood33 http://testphp.vulnweb.com/login.php USER: beruangcoklat, PASS : hibers99

From the sniffing process experiment, information was obtained that the target computer accessed http://testphp.vulnweb.com/login.php site and entered several usernames and passwords.

Banu , B., & Santoso , H. (2023). Wireless Computer Network (WLAN) Security Test at Pradita University. TEPIAN, 4(4). https://doi.org/10.51967/tepian.v4i4.2910

Overall, the implementation of wireless local area network security testing with penetration testing methods in Table 3.

Table 3. Test results

Types of Attacks	Required information	Attack Status
Cracking The Encryption	Word dictionary, other user handshakes, channels used, and BSSID of the access point.	Fail
Denial Of Service (DoS)	The attacker must be in the WLAN network, the MAC Address of the tester device.	Succeed
MITM	The attacker must be on a WLAN network, the IP address of the connected user	Succeed

the results of the attacks that have been carried out show that two attacks succeeded and one failed, indicating a gap for exploitation.

IV. Conclusion

The results of the research, it can be concluded that the WLAN Network Security test using attacks (Cracking The Encryption, Denial of Service, and MITM) at Pradita University, can be concluded that the security possessed by the Pradita University WLAN network still has many gaps to be exploited. This is evidenced by the results of the research conducted that of the three types of attacks carried out, only one has a failed status, namely the attack of cracking the encryption. The WLAN network has not been able to provide security to connected users so as not to get interference or eavesdropping from other users when accessing the same internet service. So that there is a need for regular evaluation to improve the stability and security of the WLAN network at Pradita University.

References

Agustio, D. P., and Nainggolan, E. R. (2023). Penerapan Virtual Local Area Network Pada Jaringan MAN dengan Metode Filtering Berbasis Access Control List di Dinas Komunikasi dan Informatika Kota Serang. Jurnal Komputer Antartika, 1(1), 32–38.

Boodai, J., Alqahtani, A., and Frikha, M. (2023). Review of Physical Layer Security in 5G Wireless Networks. Applied Sciences, 13(12), 72–77.

Catalano, C., Pagano, A., Piccinno, A., and Stamerra, A. (2023). Cartoons to Improve Cyber Security Education: Snow White in Browser in the Middle.

Demertzi, V., Demertzis, S., and Demertzis, K. (2023). An Overview of Cyber Threats, Attacks and Countermeasures on the Primary Domains of Smart Cities. Applied Sciences, 13(2), 790.

Haq, I. U., Ramzan, S., Ahmad, N., Ahmad, Y., and Nadeem, A. (2023). Towards Robust and Low Latency Security Framework for IEEE 802.11 Wireless Networks. International Journal of Computing and Digital Systems, 14(1).

Lutfiani, N., Wijono, S., Rahardja, U., Iriani, A., Aini, Q., and Septian, R. A. D. (2023). A bibliometric study: Recommendation based on artificial intelligence for ilearning education. Aptisi Transactions on Technopreneurship (ATT), 5(2), 109–117.

Masyhur, Z and Hartono, N. (2023). Security and Data Integrity Analysis in E-Voting Systems. Jurnal INSYPRO (Information System and Processing), 8(1).

Murumba, J. M. and Muhambe Titus, M. (2023). A Review of Smartphone as an Office: Security Risks and Mitigation Measures. setjournal.com.

Ojha, N. K., and Baray, E. (2023). An Overview of Protocols-Based Security Threats and Countermeasures in WLAN. In 2023 4th International Conference for Emerging Technology (INCET) (pp. 1–6).

Samsumar, L. D., and Gunawan, K. (2017). Analisis dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless LAN); Studi Kasus di Kampus STMIK Mataram. Jurnal Ilmiah Teknologi Infomasi Terapan, 4(1).

Samsumar, L. D., Gunawan, K. (2017). Analisis Dan Evaluasi Tingkat Keamanan Jaringan Komputer Nirkabel (Wireless Lan); Studi. Ilmiah Teknologi Informasi Terapan, IV(1), 73–82.

Saskara, G. A. J., Indrawan, I. P. O. and Putra, P. M. (2019). Keamanan Jaringan Komputer Nirkabel Dengan Captive Portal Dan Wpa/Wpa2 Di Politeknik Ganesha Guru. Jurnal Pendidikan Teknologi Dan Kejuruan, 16(2), 236–247.

Setiadi, I. H. and Afrianto, Y. (2019). Analisis Infrastruktur Jaringan Wireless Local Area Network (WLAN) PT PLN (Persero) ULP Leuwiliang. Jurnal Inovatif: Inovasi Teknologi Informasi Dan Informatika, 2(2), 174–182.

Staddon, E., Loscri, V and Mitton, N. (2023). A consensus-based approach to reputational routing in multi-hop networks. ITU Journal on Future and Evolving Technologies.

Syaputera, A., Riska and Mardiana, Y. (2023). Hotspot Network Security System From Brute Force Attack Using Pfsense External Firewall (Case Study of Wifi-Ku. Net Hotspot). Jurnal Komputer, Informasi Dan Teknologi (JKOMITEK), 3(1), 205–218.

Trungadi, P. (2023). Exploiting virtual networks for CPS security analysis--The Smart Home Environment.

Turban, E., King, D., Lee, J. K., Liang, T. Turban, D. C., Turban, E., King, D., Lee, J. K. Liang, T., and Turban, D. C. (2015). Overview of electronic commerce. In Electronic Commerce: A Managerial and Social Networks Perspective (pp. 3–49). Springer.

Widerberg, P. A., and Mattsson, W. (2023). Testing IoT

Banu , B., & Santoso , H. (2023). Wireless Computer Network (WLAN) Security Test at Pradita University. TEPIAN, 4(4). https://doi.org/10.51967/tepian.v4i4.2910

Security: A comparison of existing penetration testing frameworks and proposing a generic framework.

Xing, Y. (2023). Cyber security digital twin simulations for wireless networks. University of British Columbia.

Zen, B. P., and Saputra, S. G. (2023). Analisis Keamanan Jaringan Wireless menggunakan Metode Penetration Testing Execution Standard (PTES). Jurnal Sistem Informasi Galuh, 1(2).