JPPIPA 9(12) (2023)

Jurnal Penelitian Pendidikan IPA

Journal of Research in Science Education

http://jppipa.unram.ac.id/index.php/jppipa/index

Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators

Tamsir Ariyadi[1*], M. Rizky Pohan[1]

[1] Department of Computer Engineering, Universitas Bina Darma, Palembang, Indonesia.

Received: October 3, 2023
Revised: November 9, 2023
Accepted: December 20, 2023
Published: December 31, 2023

Corresponding Author:
Tamsir Ariyadi
tamsirariyadi@binadarma.ac.id

DOI: 10.29303/jppipa.v9i12.5551

Abstract: Wi-Fi networks have become a critical infrastructure in many organisations, including the Directorate of Innovation and Business Incubator. However, potential vulnerabilities in Wi-Fi networks also increase as technology advances. Therefore, testing is needed to identify and address security that can harm network users. This research aims to implement penetration testing tools in testing the security level of Wi-Fi networks at the Directorate of Innovation and Business Incubator. The penetration testing method is used to test security and assess the level of resistance to attacks on Wi-Fi in the form of simulated attacks. One of the operating systems that provides penetration testing tools that meet the needs of testing is linux times. The tools used in the penetration testing process are airmon-ng, airodump-ng, aireplay-ng, aircrack-ng, macchanger, ettercap and wireshark. The results showed that the Wi-Fi security of the Directorate of Innovation and Business Incubator still needs to be improved where the results of the four types of attacks only one failed, namely MAC Spoofing. In addition, the tests on Denial of Service, Cracking the Encryption, and Man-in-the-Middle attacks were successful. The application of anticipation by increasing Wi-Fi security based on the attacks that have been carried out can prevent these attacks.

Keywords: Kali linux; Penetration testing; Security; Tool; Wi-Fi

Introduction

In the increasingly rapidly developing digital era, wireless connectivity, especially Wi-Fi networks, has become important infrastructure in various organizations (Efe et al., 2019). Wi-Fi (Wireless Fidelity) is a technology that allows electronic devices, such as computers, smartphones, or tablets, to connect to an internet network or local network (LAN) without using physical cables. Wi-Fi uses IEEE 802.11 standard technology to transmit data via radio waves, which allows practical and efficient internet access and wireless communications (Suroto, 2018). Wi-Fi provides easy internet access needed by staff, students, visitors and various devices connected to the network, all of which play an important role in supporting daily activities and innovation at the Directorate of Innovation and Business Incubators (DIIB).

However, the existence of a Wi-Fi network does not escape cyber-attacks carried out by irresponsible parties which can result in harm to other people (Adiguna et al., 2022). Based on data from the National Cyber and Crypto Agency (BSSN) in 2022, Indonesia recorded around 370.02 million cyber-attack incidents. This figure shows an increase of 38.72% from the previous year, where around 266.74 million cyber-attacks were recorded in Indonesia (Pratiwi, 2022). Therefore, Wi-Fi network security is crucial considering the large amount of sensitive data and confidential information that can be accessed via this network. Security threats such as hacking, data theft and attacks of various types increasingly intensify the need to protect Wi-Fi (Adiguna et al., 2022).

The Directorate of Innovation and Business Incubator (DIIB) is a directorate at Bina Darma University that focuses on developing innovation and

How to Cite:
Ariyadi, T., & Pohan, M. R. (2023). Implementation of Penetration Testing Tools to Test Wi-Fi Security Levels at the Directorate of Innovation and Business Incubators. *Jurnal Penelitian Pendidikan IPA*, *9*(12), 10768–10775. https://doi.org/10.29303/jppipa.v9i12.5551

providing support for business growth from student and lecturer innovation. DIIB also uses the Wi-Fi network as infrastructure to help meet information needs such as accessing the internet, opening social media, carrying out online transactions and the like. The Wi-Fi network provided by the Directorate of Innovation and Business Incubators has implemented the WPA2-PSK security system on the access points used to connect to the network. However, using WPA2-PSK security alone on Wi-Fi without any additional security configuration still has many loopholes that can be exploited with the increasing level of complexity of cyber-attacks and the variety of techniques used by attackers, this is very dangerous for Wi-Fi network users in DIIB because it does not rule out the possibility of attacks on the network.

Based on the problems above, identifying security weaknesses in the network is an important step to deal with existing threats (Singh et al., 2017). In this case, penetration testing is an effective method for testing and exposing security weaknesses in a system or network (Wahyudi et al., 2019). Penetration testing on Wi-Fi involves a deliberate effort to test the security of a wireless network using techniques and methods similar to attacks that can be carried out by attackers such as Denial of Service, Password Cracking, Spoofing, and Man in the Middle (MITM) attacks (Saraun et al., 2022).

In carrying out penetration testing, the use of various tools is key in simulating attacks to test the security level of a system or network. To carry out effective penetration testing on Wi-Fi networks, tools are needed that have various functionalities, such as network scanning, exploitation and monitoring (Kongara, 2023). Kali Linux is a Linux distribution specifically developed for penetration testing and computer security purposes (Rusdi et al., 2019). Kali Linux provides many tools and applications that are integrated by default to support penetration testing activities. In it, there are various important tools that are ready to be used to carry out penetration testing on Wi-Fi networks such as aircrack-ng, wireshark and other tools (Kyei et al., 2020).

This research aims to implement penetration testing tools to test the level of Wi-Fi network security applied at the Directorate of Innovation and Business Incubator, especially in facing the threat of cyber-attacks that have the potential to disrupt and harm users (Abdulqader et al., 2016). In this research, penetration testing will be carried out by simulating several types of attacks, including Denial of Service, Cracking the Encryption, MAC Spoofing, and Man-in-the-Middle using tools available in the Kali Linux operating system (Gunawan et al., 2018). Thus, this research specifically aims to determine potential security gaps that can be exploited by various wireless network attacks that have the potential to threaten the Wi-Fi used by the Directorate of Innovation and Business Incubators.

Previous research has carried out a lot of penetration testing to test the security of Wi-Fi networks. For example, research by Lu et al. (2021) shows experimental results that the Wi-Fi network penetration testing method with Kali Linux has a good effect in improving Wi-Fi network security evaluation. Research conducted by Prakosa (2020) also identified common attacks on Wi-Fi networks by using penetration testing methods and providing data as material to strengthen network security.

Method

The research method used is the penetration testing method which refers to the NIST SP 800-115 standard (Astriani, 2021). According to Alamanni (2015) the penetration testing method is a method that simulates attacks on a system or network to identify configuration errors, vulnerabilities or security violations and related exploits that can be used by real attackers to gain access to a system or network. The NIST SP 800-115 penetration testing method consists of several stages, namely the planning, discovery, attack, and reporting stages (Santoso et al., 2022).

Figure 1. NIST SP 800-115 method

Table 1. Tools Penetration Testing

Attack	Tool	Version
Denila of service	Airmon-ng	1.7
	Airodump-ng	1.7
	Aireplay-ng	1.7
Cracking the Encryption	Airmon-ng	1.7
	Airodump-ng	1.7
	Aireplay-ng	1.7
	Aircrack-ng	1.7
MAC Spoofing	Airmon-ng	1.7
	Airodump-ng	1.7
	Macchanger	1.7.0
Man-in-the-Middle	Ettercap	0.8.3.1
	Wireshark	4.0.7

This research requires the kali linux operating system to perform penetration testing on Wi-Fi networks (Ariyadi et al., 2023). The kali linux operating

system is specifically designed for penetration testing purposes and has various tools that can be used to test network security (Sitompul et al., 2023). The penetration testing tool that will be used in this research is based on the evaluation of attacks that will be carried out on the Wi-Fi network of the Directorate of Innovation and Business Incubator.

In this test, several test steps and their explanations, as for the flowchart image of the testing technique can be seen in Figure 2.

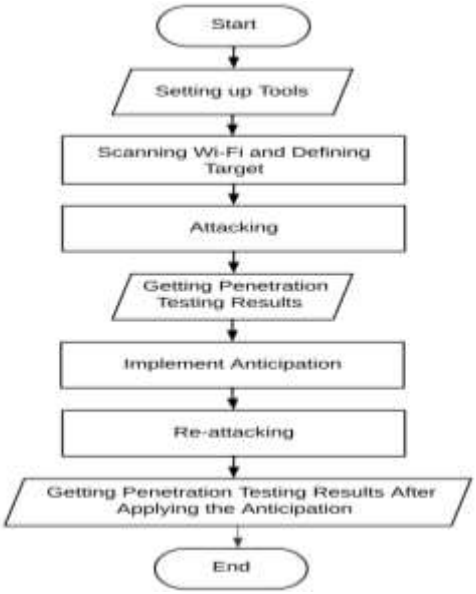

Figure 2. Flowchart

The first step in the testing flow is to prepare penetration testing tools that will be used in testing and ensure that the tools are ready to use and in accordance with research needs. Next, scanning the Wi-Fi network and determining the target to be tested (Bertoglio et al., 2017). After scanning, then carry out attacks using penetration testing tools that are suitable for testing Wi-Fi network security. From this process will get the results of a successful attack (Malgaonkar et al., 2017). After getting the results of penetration testing, the researcher will apply anticipation of a successful attack. Furthermore, re-attack the network that has been applied anticipation. From all the processes that have been carried out, we will get the overall results of each testing process (Wang et al., 2016).

The researcher collected information about the network topology, devices used, existing security and analysed the information found to identify potential vulnerabilities that may exist in the system on the Directorate of Innovation and Business Incubator's Wi-Fi network.

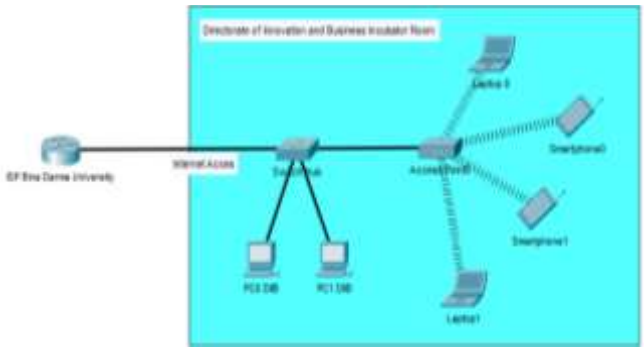

Figure 3. Network topology

Table 2. Vulnerability analysis

Vulnerability	Information	Potential Attacks Identified
No Firewall	No firewall that enforces network traffic control or access rules	Potential Denial of Service (DoS) attacks, spoofing
Configuration Weaknesses	The use of WPA2-PSK encryption, which is the encryption standard on Wi-Fi networks, still has loopholes for cracking.	Potential cracking the encryption attacks
Authentication Weaknesses	Use of weak authentication or still using automatic authentication mechanisms on user devices	Potential attack of cracking the encryption, making it easier for attackers to get the WPA key
Weaknesses of MAC filtering	No MAC restrictions on devices connected to the network	Potential unauthorised access, MAC Spoofing
Lack of Monitoring	No monitoring of network traffic or suspicious activity	Potential man-in-the-middle attack
Lack of Security Awareness	Unwary users use Wi-Fi networks to access the internet related to important data	Potential man-in-the-middle attacks, data theft

In Figure 3 the Directorate of Innovation and Business Incubator room uses a switch to connect computers in the room using a LAN cable and an access point that emits signals to connect devices such as laptops, smartphones, and others wirelessly in order to access the internet. The penetration test targets in this research are access points and devices connected to the wireless network. The Wi-Fi network system running at the Directorate of Innovation and Business Incubator uses the WPA2-PSK (Wi-Fi Protected Access 2 Pre-

Shared Key) security system with the default configuration on the access point (Indira Reddy et al., 2019). WPA2-PSK security is a security mechanism used to protect Wi-Fi networks from attacks and unauthorized access. WPA2-PSK uses symmetric encryption using a pre-shared key, also known as a passphrase or password (Chang et al., 2019).

Researchers conducted information searches and identified a number of vulnerabilities in Wi-Fi networks that would be used as a basis for testing attacks (Goel et al., 2015). The results of the vulnerability analysis conducted by researchers can be seen in table 2.

Result and Discussion

This stage is the core stage in the research where researchers will simulate Denial of Service (DoS), Encryption Cracking, MAC Spoofing, and Man-in-the-Middle (MITM) attacks based on the results of the discovery stage using the tools and flow that have been determined at the planning stage (Waliullah et al., 2014).

The results of denial-of-service attacks using the tools airmon-ng, airodump-ng, and aireplay-ng. In the results of the attack, the Wi-Fi network of the Directorate of Innovation and Business Incubator can still be attacked by sending a deauthentication frame to the access point so that users cannot connect to the network until the attack is stopped or the deauthentication frame is no longer sent (Cetinkaya et al., 2019). This is because the deauthentication frame is used in Wi-Fi networks to forcibly disconnect the connection between the device and the access point can be seen in the figure 4.

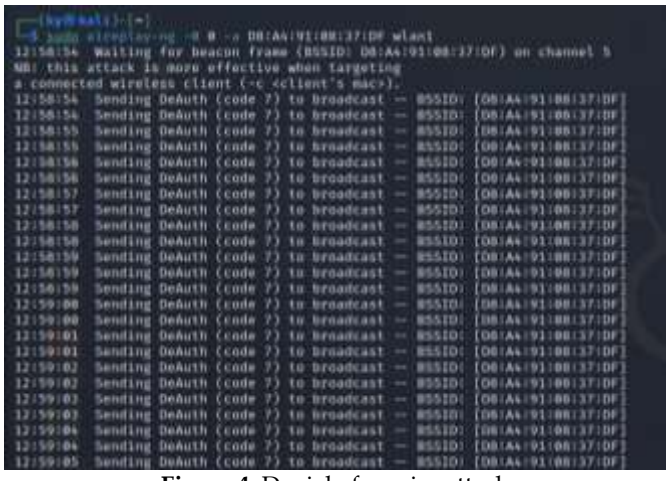

Figure 4. Denial of service attack

The results of the encryption cracking attack using the tools airmon-ng, airodump-ng, aireplay-ng, and aircrack-ng were successful. This attack poses a serious potential risk to network security and data privacy that must be strictly maintained. In the results of the attack, the Wi-Fi network encryption security of the Directorate of Innovation and Business Incubator can still be cracked using brute force techniques to break the WPA key encryption with the aim of obtaining the password that has been applied to the access point. The results of this attack reveal that the security system used, in this case the WPA key encryption, is not strong enough to protect the network from brute force attacks (Bosnjak et al., 2018).

Figure 5. Result cracking the encryption

The results of the MAC spoofing attack using the airmon-ng, airodump-ng, and macchanger tools. In the results of this attack, researchers were unable to connect to a Wi-Fi network using the MAC address of a device that was already connected to the network. This is because the access point cannot provide connection access to two MAC addresses of the same device. This attack was successful when the device left the network. This suggests that Wi-Fi network security is well organised in terms of managing connected devices (Vaidya et al., 2016). These results show the importance of careful device management in Wi-Fi networks, as well as the ability of access points to detect and restrict unauthorised access. At the same time, however, the results also show that this kind of attack still has the potential to be costly if proper precautions are not taken.

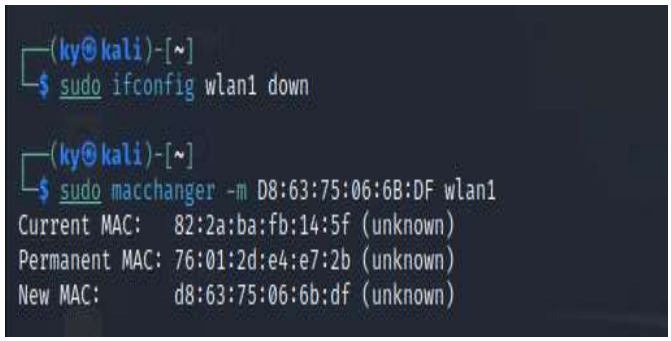

Figure 6. MAC spoofing

The results of man-in-the-middle attacks using ettercap and wireshark tools. In the results of the attack successfully obtained sensitive user login information with sniffing techniques using ettercap (Prabadevi et al.,

2018). This attack can sniff websites with HTTP and HTTPS protocols combined with SSLstrip which can downgrade the HTTPS protocol to HTTP.

From the overall results, this testing activity was carried out in order to determine the level of security of the Wi-Fi network at the Directorate of Innovation and Business Incubator. In the penetration testing process, researchers conducted four types of attacks, namely denial of service, cracking the encryption, MAC spoofing, and man-in-the-middle using penetration testing tools. The results of all attack processes can be seen in table 3.

Figure 7. Man-in-the-Middle attack

Table 3. Penetration Testing Result

Attack type	Required information	Tools used	Status	Description
Denial of Service	Channel and BSSID access point	Airmon-ng, Airodump-ng, Aireplay-ng	Success	Successfully disconnect Wi-Fi
Cracking the Encryption	Channel and BSSID access point, Handshake user, Database wordlist	Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng	Success	Successfully obtained Wi-Fi password
MAC Spoofing	MAC address of the user connected to the network	Airmon-ng, Airodump-ng, Macchanger	Fail	Failed to connect to Wi-Fi network with fake MAC
Man-in-the-Middle	IP address access point and IP address user	Ettercap, Wireshark	Success	Successfully get user data both HTTP and HTTPS protocols

After conducting a series of tests on the security conditions of the existing Wi-Fi network at the Directorate of Innovation and Business Incubator, researchers have successfully identified various vulnerabilities and weak points in the network infrastructure. These results are the basis for ongoing anticipation to increase the level of Wi-Fi network security from attacks that could potentially threaten network users (Etta et al., 2022). The security improvements that will be implemented based on the results of the penetration testing that has been carried out can be seen in table 4.

Table 4. Implement Anticipation

Improvement	Description
Firewall Configuration	Enable the firewall feature on the access point
WPA3 Encryption Configuration	Use better encryption and provide a password with a length of 15 characters, a combination of uppercase letters, lowercase letters, numbers and symbols.
MAC filtering whitelist configuration	Allows only registered MACs to connect to the network.
AP Isolation Configuration	Restricts communication between hosts on the same network

The next step is testing after applying anticipation, this is done to find out whether the retest produces different results from the results that have been carried out in security testing on the Wi-Fi network of the Directorate of Innovation and Business Incubator. The retesting process is carried out exactly the same as the previous test by carrying out four types of attacks, namely denial of service, cracking the encryption, MAC spoofing, and man-in-the-middle using penetration testing tools. From all the processes carried out, the improvement status can be seen in table 5. This table provides a clear picture of whether the implemented corrective actions are successful in increasing the level of network security (Mekhaznia et al., 2015).

Table 5. Penetration Testing Result after Applying Anticipation

Attack type	Required information	Tools used	Status	Description
Denial of Service	Channel and BSSID access point	Airmon-ng, Airodump-ng, Aireplay-ng	Fail	Unsuccessfully disconnecting Wi-Fi
Cracking the Encryption	Channel and BSSID access point, Handshake user, Database wordlist	Airmon-ng, Airodump-ng, Aireplay-ng, Aircrack-ng	Fail	Unsuccessful in obtaining Wi-Fi password
MAC Spoofing	MAC address of the user connected to the network	Airmon-ng, Airodump-ng, Macchanger	Fail	Failed to connect to Wi-Fi network with fake MAC
Man-in-the-Middle	IP address access point and IP address user	Ettercap, Wireshark	Fail	Unable to get IP Address during scanning

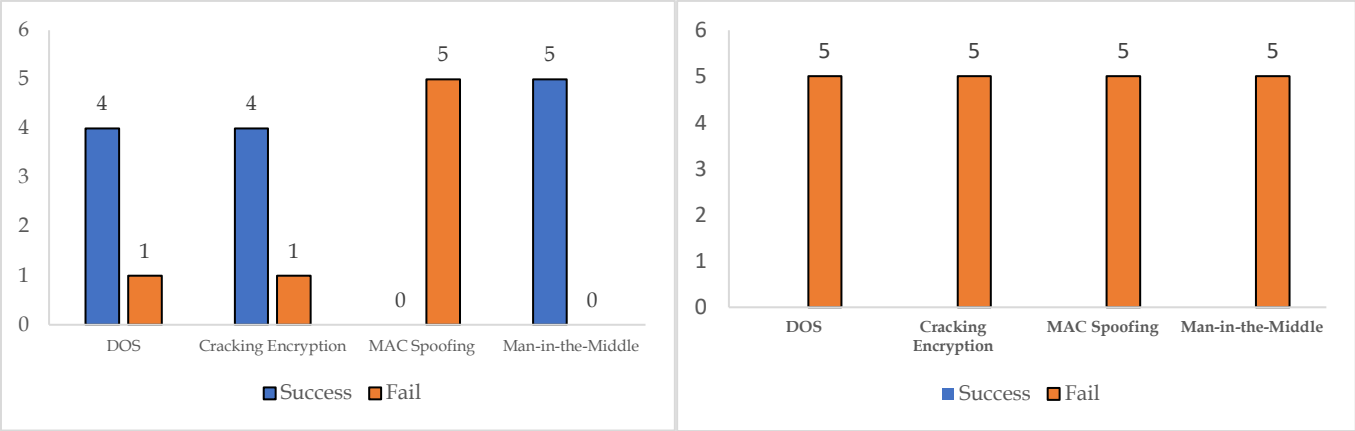

Figure 8. Comparison of testing before and after implementing anticipation

In Figure 8, the denial of service, encryption cracking, MAC spoofing, and man-in-the-middle attacks were tested 5 times each. From the diagram, it can be seen that the denial of service attack has a high scale with 4 successful attacks and 1 failure. The encryption cracking attack was also successfully carried out 4 times and 1 failure, the MAC spoofing attack has a fairly small scale with 1 success and 4 failures. The man-in-the-middle attack was successfully carried out 5 times without failure, so it has the highest scale of other attacks (Alsahlany et al., 2018).

In Figure 8, denial of service, encryption cracking, MAC spoofing, and man-in-the-middle attacks were tested 5 times each. From the diagram, it can be seen that by increasing the security of attacks such as denial of service is successfully prevented without any successful attack attempts, these results have a high scale. The encryption cracking attack after improving encryption security successfully counteracted the cracking attack 5 times this result shows a very good improvement (Haque et al., 2020). MAC spoofing and man-in-the-middle attacks also have a very good scale, where all attack attempts cannot be successfully carried out after increasing security on the Wi-Fi network.

Conclusion

Based on research on Wi-Fi network security testing that has been carried out at the Directorate of Innovation and Business Incubator using penetration testing tools, it can be concluded that Wi-Fi network security at the Directorate of Innovation and Business Incubator needs to be improved. This is evidenced by Denial of Service, Cracking the encryption and Man-in-the-Middle attacks that can be exploited using penetration testing tools. Denial of Service attacks cause all devices connected to the Wi-Fi network to be disconnected and unable to connect to the network. This attack can be anticipated by implementing a firewall and WPA3 security. Cracking the encryption attack causes the password on the access point to be found or cracked with brute force techniques. This attack can be anticipated by implementing WPA3 encryption and complex password combinations. The application of whitelist MAC filtering on access points has a positive impact on network users because it makes it difficult for attackers to connect to the network with fake MAC addresses. Man-in-the-Middle attacks are successful in obtaining important target data and important information about users. This attack can be anticipated by implementing AP isolation on the access point, by limiting communication between users can avoid potential Man-in-the-Middle attacks.

Acknowledgments
The author would like to thank the supervisors from the Computer Engineering Department of Bina Darma University for the knowledge and financial support provided in this research.

Author Contributions
Authors listed in this article contributed to the research and development of the article.

Funding
This research uses the author's personal funds.

Conflicts of Interest
In writing this article, we sincerely declare that there are no conflicts of interest that may affect the objectivity and integrity of the results.

References

Abdulqader, M. F., & Y. Dawod, A. (2016). Penetration Testing of Wireless Networks. *Kirkuk University Journal-Scientific Studies*, *11*(3), 136–151. https://doi.org/10.32894/kujss.2016.124737

Adiguna, M. A., & Widagdo, B. W. (2022). Analisis Keamanan Jaringan WPA2-PSK Menggunakan Metode Penetration Testing (Studi Kasus : Router Tp-Link Mercusys Mw302r). *Jurnal SISKOM-KB*

(Sistem Komputer Dan Kecerdasan Buatan), *5*(2), 1–8. https://doi.org/10.47970/siskom-kb.v5i2.268

Alamanni, M. (2015). Kali Linux Wireless Penetration Testing Essentials. In *Community experience distilled*.

Alsahlany, A. M., Alfatlawy, Z. H., & Almusawy, A. R. (2018). Experimental evaluation of different penetration security levels in wireless local area network. *Journal of Communications*, *13*(12), 723–729. https://doi.org/10.12720/jcm.13.12.723-729

Ariyadi, T., Widodo, T. L., Apriyanti, N., & Kirana, F. S. (2023). Analisis Kerentanan Keamanan Sistem Informasi Akademik Universitas Bina Darma Menggunakan OWASP. *Techno.Com*, *22*(2), 418–429. https://doi.org/10.33633/tc.v22i2.7562

Astriani, T. (2021). Analisa Kerentanan Pada Vulnerable Docker Menggunakan Scanner Openvas Dan Docker Scan Dengan Acuan Standar Nist 800-115. *JATISI (Jurnal Teknik Informatika Dan Sistem Informasi)*, *8*(4), 2041–2050. https://doi.org/10.35957/jatisi.v8i4.1232

Bertoglio, D. D., & Zorzo, A. F. (2017). Overview and open issues on penetration test. *Journal of the Brazilian Computer Society*, *23*(1), 1–16. https://doi.org/10.1186/s13173-017-0051-1

Bosnjak, L., Sres, J., & Brumen, B. (2018). Brute-force and dictionary attack on hashed real-world passwords. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2018 - Proceedings*, *February*, 1161–1166. https://doi.org/10.23919/MIPRO.2018.8400211

Cetinkaya, A., Ishii, H., & Hayakawa, T. (2019). An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy*, *21*(2), 1–29. https://doi.org/10.3390/e21020210

Chang, T. H., Chen, C. M., Hsiao, H. W., & Lai, G. H. (2019). Cracking of wpa & wpa2 using gpus and rule-based method. *Intelligent Automation and Soft Computing*, *25*(1), 183–192. https://doi.org/10.31209/2018.100000054

Efe, A., & Kaplan, M. B. (2019). Multidisciplinary Studies and Innovative Technologies Wi-Fi Security Analysis For E & M-Government Applications. *Nternational Journal of Multidisciplinary Studies and Innovative Technologies*, *3*(2), 86–98. Retrieved from https://dergipark.org.tr/en/pub/ijmsit/issue/50263/617035

Etta, V. O., Sari, A., Imoize, A. L., Shukla, P. K., & Alhassan, M. (2022). Assessment and Test-case Study of Wi-Fi Security through the Wardriving Technique. *Mobile Information Systems*, *2022*. https://doi.org/10.1155/2022/7936236

Goel, J. N., & Mehtre, B. M. (2015). Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology. *Procedia Computer Science*, *57*, 710–715. https://doi.org/10.1016/j.procs.2015.07.458

Gunawan, T. S., Lim, M. K., Kartiwi, M., Malik, N. A., & Ismail, N. (2018). Penetration testing using Kali linux: SQL injection, XSS, wordpres, and WPA2 attacks. *Indonesian Journal of Electrical Engineering and Computer Science*, *12*(2), 729–737. https://doi.org/10.11591/ijeecs.v12.i2.pp729-737

Haque, A., Raj, N., Sinha, A. K., & Singh, N. K. (2020). *Wi-Fi Ado ption And Security Surv ey*. *July 2017*. https://doi.org/10.9790/1676-1204016774

Indira Reddy, B., & Srikanth, V. (2019). Review on Wireless Security Protocols (WEP, WPA, WPA2 & WPA3). *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, *5*(4), 28–35. https://doi.org/10.32628/cseit1953127

Kongara, D. (2023). A Process of Penetration Testing Using Various Tools. *Mesopotamian Journal of Cyber Security*, *August*, 94–104. https://doi.org/10.58496/mjcs/2023/014

Kyei, M., & Asante, M. (2020). Penetration Testing of IEEE 802.11 Encryption Protocols using Kali Linux Hacking Tools. *International Journal of Computer Applications*, *176*(32), 26–33. https://doi.org/10.5120/ijca2020920365

Lu, H. J., & Yu, Y. (2021). Research on WiFi Penetration Testing with Kali Linux. *Complexity*, *2021*. https://doi.org/10.1155/2021/5570001

Malgaonkar, S., Patil, R., Rai, A., & Singh, A. (2017). Research on Wi-Fi Security Protocols. *International Journal of Computer Applications*, *164*(3), 30–36. https://doi.org/10.5120/ijca2017913601

Mekhaznia, T., & Zidani, A. (2015). Wi-Fi Security Analysis. *Procedia Computer Science*, *73*(Awict), 172–178. https://doi.org/10.1016/j.procs.2015.12.009

Prabadevi, B., & Jeyanthi, N. (2018). A review on various sniffing attacks and its mitigation techniques. *Indonesian Journal of Electrical Engineering and Computer Science*, *12*(3), 1117–1125. https://doi.org/10.11591/ijeecs.v12.i3.pp1117-1125

Prakosa, B. A. (2020). Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method. *Jurnal Mantik*, *4*(3), 1658–1662. https://doi.org/10.35335/mantik.Vol4.2020.974.pp1658-1662

Pratiwi, F. S. (2022). *BSSN Catat 370,02 Juta Serangan Siber ke Indonesia pada 2022*. Dataindonesia.Id. Retrieved from https://dataindonesia.id/internet/detail/bssn-

cata

Rusdi, M. I., & Prasti, D. (2019). Penetration Testing Pada Jaringan Wifi Menggunakan Kali Linux. *Seminar Nasional Teknologi Informasi Dan Komputer 2019*, 260–269. Retrieved from https://journal.uncp.ac.id/index.php/semantik/article/view/1524

Santoso, N. A., Ainurohman, M., & Kurniawan, R. D. (2022). Penerapan Metode Penetrasion Testing Pada Keamanan Jaringan Nirkabel. *Jurnal Responsif: Riset Sains Dan Informatika*, *4*(2), 162–167. https://doi.org/10.51977/jti.v4i2.831

Saraun, A., Lumenta, A. S. M., & Sengkey, D. F. (2022). Analisa Keamanan Jaringan Nirkabel IEEE 802.11 pada Kantor Dinas Pendidikan Kabupaten Minahasa. *Jurnal Teknik Informatika*, *17*(1), 565–572. https://doi.org/10.35793/JTI.17.1.2022.35321

Singh, H., & Singh, J. (2017). Penetration Testing In Wireless. *International Journal of Advanced Research in Computer Science*, *8*(5), 2213–2216. https://doi.org/10.26483/ijarcs.v8i5.4012

Sitompul, A. T., Chahyadi, F., Informatika, J. T., Teknik, F., Maritim, U., & Ali, R. (2023). Analisis Penerapan Metode Penetration Testing pada Keamanan Jaringan Wlan (Studi Kasus: Universitas Maritim Raja Ali Haji). *Jurnal Hasil Penelitian Dan Industrii Terapan*, *12*(01), 23–29. Retrieved from http://repositori.umrah.ac.id/3842/

Suroto. (2018). Wlan security: Threats and countermeasures. *International Journal on Informatics Visualization*, *2*(4), 232–238. https://doi.org/10.30630/joiv.2.4.133

Vaidya, A., Jaiswal, S., & Motghare, M. (2016). A review paper on spoofing detection methods in wireless LAN. *Proceedings of the 10th International Conference on Intelligent Systems and Control, ISCO 2016*, *January 2016*. https://doi.org/10.1109/ISCO.2016.7727054

Wahyudi, E., & Efendi, M. M. (2019). Wireless Penetration Testing Method To Analyze WPA2-PSK System Security And Captive Portal. *Explore*, *9*(1), 1. https://doi.org/10.35200/explore.v9i1.32

Waliullah, M., & Gan, D. (2014). Wireless LAN Security Threats & Vulnerabilitiess: A Literature Review. *(IJACSA) International Journal of Advanced Computer Science and Applications*, *5*(1), 176–183. Retrieved from https://rb.gy/1hv38i

Wang, S.-L., Wang, J., Feng, C., & Pan, Z.-P. (2016). Wireless Network Penetration Testing and Security Auditing. *ITM Web of Conferences*, *7*, 03001. https://doi.org/10.1051/itmconf/20160703001