Jurnal Mantik
Volume 4, Number 3, Nov 2020, pp. 1658-1662 E-ISSN 2685-4236
https://iocscience.org/ejournal/index.php/mantik

Security Analysis of Wireless Local Area Network (WLAN) Network with the Penetration Testing Method

Fikriyadi[1], Ritzkal[2], Bayu Adhi Prakosa[3].

[1,2,3]Technical Information, Faculty Of Engineering And Sanis, Ibn Khaldun University Bogor,Indonesia

E-mail: fikrie.yee@gmail.com[1], ritzkal@ft.uika-bogor.ac.id[2] ,bayu.adhi@ft.uika-bogor.ac.id [3]

ARTICLE INFO

Article history:
Received: 12/07/2020
Revised: 22/08/2020
Accepted: 30/09/2020

Keywords:
Penetration Testing, Wireless LAN, Security Systems

ABSTRACT

Wireless Local Area Network (WLAN) is an alternative in overcoming cabling problems in a local network. Often wireless network security that is installed still uses vendor default settings such as SSID, IP Address, remote management, DHCP enabled, frequency channels, without encryption, even user or password for wireless administration. How does a strong WLAN security system work? The most common security system applied to wireless networks at this time is starting from securing access points by applying the MAC Filtering concept, using WPA / WPA2-PSK security keys, and RADIUS server authentication. To see the quality of wireless LAN network security, how do you analyze the test of the existing security system in the network. The method that can be used in evaluating wireless networks is by testing the system by simulating forms of attacks on wireless networks with the Penetration Testing method. By carrying out 4 stages of research using the penetration testing method (i) the planning stage, (ii) the discovery stage, (iii) the attack stage and (iv) the report stage, from the attack stage (Cracking The Encryption, Bypassing MAC Address, Attacking The Infrastructure and MITM) using Kali Linux got the results of four types of attacks carried out, only one of which was failed, namely the cracking attack type of the encryption on the RADIUS server due to using captive portal authentication.

1. Introduction

With the wireless technology, a person can move or do activities anywhere and anywhere to communicate data. Wireless network is a wireless computer network technology, which uses high-frequency waves. So that the computers can be connected to each other without using cables. Even though there is convenience from wireless technology, it turns out that wireless networks have weaknesses compared to wired networks including security. Weaknesses of wireless networks can generally be divided into 2 types, namely weaknesses in configuration and weaknesses in the type of encryption used. One example of the causes of weakness in the configuration is because currently building a wireless network is quite easy. Many vendors provide facilities that make it easier for users or network admins, so it is often found that wireless is still using the vendor's default wireless configuration. Often wireless installed on the network still uses vendor default settings such as SSID, IP address, remote management, DHCP enabled, frequency channels, without encryption, even the user or password for wireless administration [1]. Therefore, security on networks that use technology wireless must be maximal. To see the quality of wireless LAN network security, it is necessary to analyze the existing security system in the network. One method that can be used in evaluating a wireless network is by testing the system by simulating forms of attacks on wireless networks or what is commonly known as the Penetration Testing method [2].

In analyzing the security of a wireless LAN network with the Penetration Testing method where the form of attack on a wireless network simulates, one of the operating systems that has the right specifications is Kali Linux. Unlike other Linux distributions, such as Ubuntu which prioritizes user friendly and balancing aspects, Kali Linux is specially designed for network security testing, equipped with supporting applications used in hacking activities and using it as a network security testing tool [3]. The formulation of the problems in this study are (1) How does a Wireless Local Area Network (WLAN) network security system work? (2) How to test a Wireless Local Area Network (WLAN) network security system by means of Penetration Testing? Based on the formulation of these problems, the objectives of this study are: (1) Knowing how the Wireless Local Area Network (WLAN) network security system works, (2) Testing the Wireless Local Area Network (WLAN) network security system by means of penetration testing.

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

2. Research Method

The research method used is the Penetration Testing method. Penetration Testing (Pentest) is an activity where someone tries
simulate attacks that can be done against a particular organization / company network to find weaknesses in the network system. People who do this activity are called Penetration Tester abbreviated as Pentester [3].
The following are the stages of implementation in research, so that each research objective is obtained.

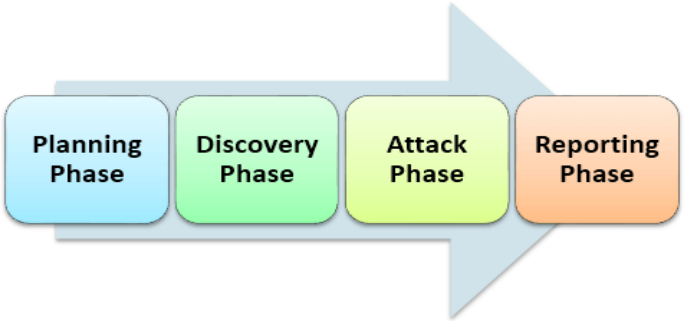

Fig 1. Research Method[4]

3. Result

3.1 Planning Phase

In designing a security model, it is necessary to pay attention to the network assets that are at risk of any potential weaknesses, who the attacker might cause interference, and the motivation of carrying out the attack for each of the existing potential weaknesses. An analysis of these matters is required to take the appropriate security protective measures as needed. Analysis of this can be seen in Table 1

Table 1
Wireless LAN security analysis

Potential Weaknesses.	Attacker.	Motivation / Purpose.	Assets at risk.	Type of Attack.
Autentikasi sistem	*Unauthorized wireless user*	Steal data, access the internet	*Access point, jaringan internal, wireless user*	*Attack* terhadap kunci enkripsi
Control Access	*Unauthorized wireless user*	Steal data, access the internet	*Access point, jaringan internal, wireless user*	*MAC address spoofing*
Data confidentiality	*Unauthorized wireless user* and *authorized wireless user*	Steal data, cause interference and loss	*Access point, jaringan internal, wireless user*	*Man In The Midde Attack*
Data Integrity	*Unauthorized wireless user*	Cause disturbances and losses	*Access point, jaringan internal, wireless user*	*Denial Of Service Attack*
System Availability	*Unauthorized wireless user* and *authorized wireless user*	Cause disturbances and losses	*Access point, wireless user*	*Denial Of Service Attack*

In Table 1, what is meant by authorized wireless user is a user who already has access and has connected to the wireless LAN network, both in the form of users who do have a valid login and password (legitimate wireless user) or users who have successfully entered the network without has a valid login (stealing login identity or stealing a session). Meanwhile, what is meant by unauthorized wireless user are people who do not have access or who have not connected to the wireless LAN. An attack carried out by an unauthorized wireless user means that the attack can occur even if the attacker has not connected to the

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

Wireless LAN. This is possible because of the characteristics of a wireless LAN network that uses the air medium as data transmission so that anyone can capture ongoing communications (passive snooping). Meanwhile, an attack carried out by an authorized wireless user requires an incoming connection to the wireless LAN, and can be carried out by someone who does have a login (legitimate wireless user) or by someone who does not have a login (by stealing an identity or session).

3.2 Discovery Phase

This stage begins with data collection by scanning the wireless local area network. The data obtained from the next stage is then analyzed. These activities include:

a) Wireless network identification.

b) Determine the target of attacks on the access point.

At the scanning and packet capture stage requires some basic information, namely SSID, BSSID, Channel. The tools used in packet capturing are airmon-ng and airodump-ng

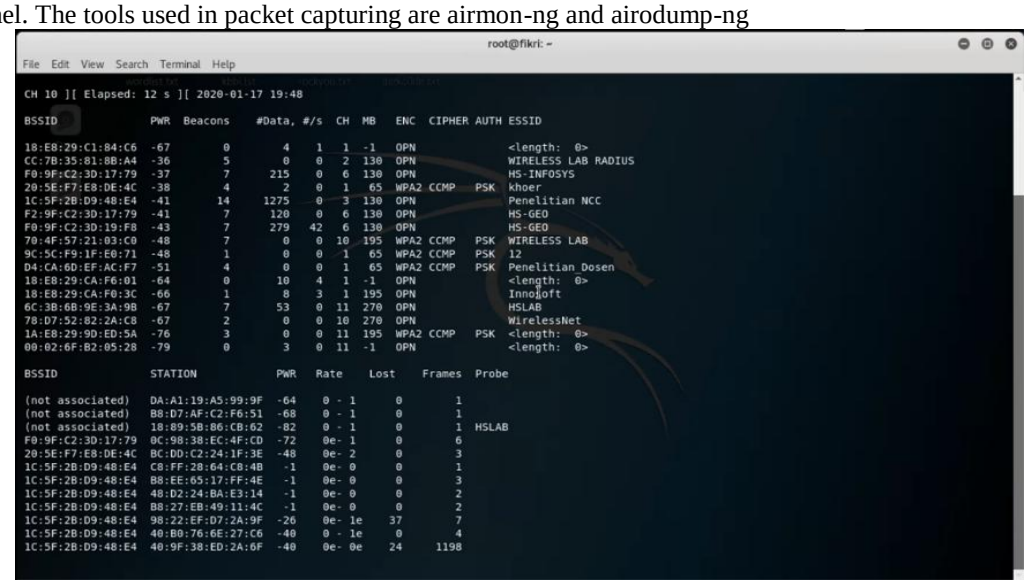

Fig 2. Detected wireless network information

3.3 Attack Phase

Analysis of cracking the encryption testing using the Wireshark application. The results of the capture of the wireshark when the attack is carried out can be seen in Figure 3 This happens when the attacker performs a deauthentication attack, namely the attacker sends a deauthentication packet that disrupts the wireless service to the user, so that the user connection associated with the AP is lost. A deauthentication attack is used by attackers to obtain data regarding wireless authentication. This data is only obtained at the beginning of the user communication with the AP. The attacker performs a deauthentication attack to speed up getting this data by disconnecting and forcing the user's device to reconnect with the AP.

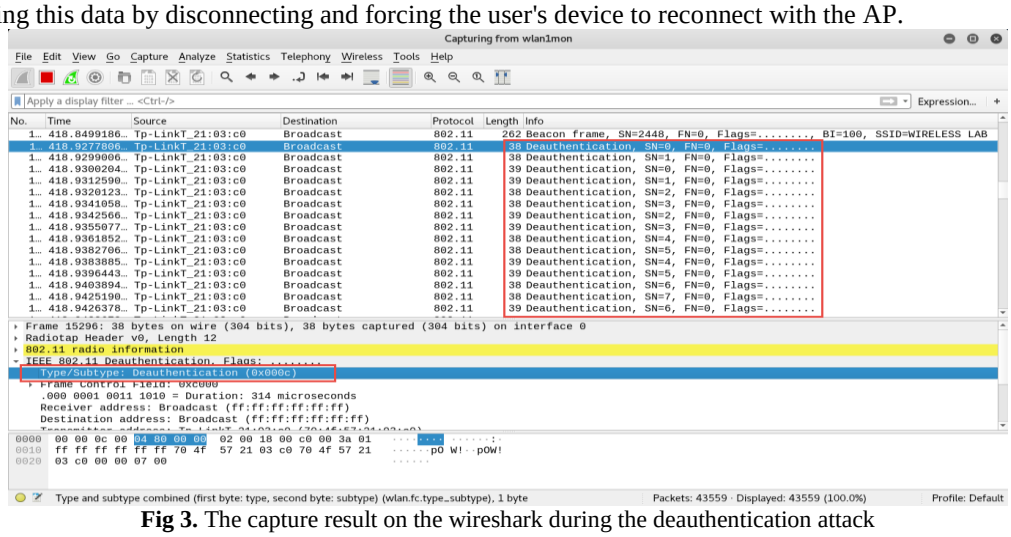

Fig 3. The capture result on the wireshark during the deauthentication attack

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

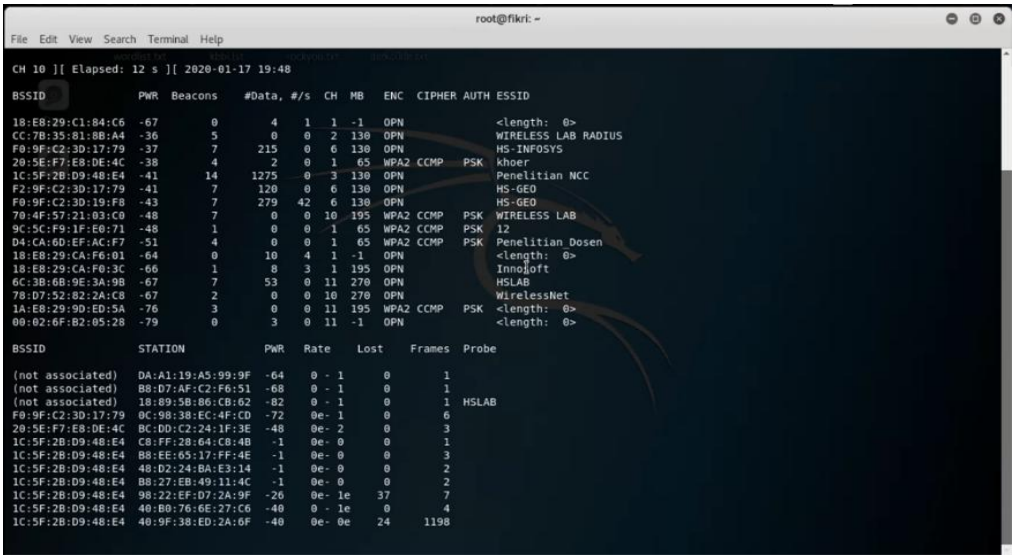

Fig 4. Capture result on EAPOL wireshark protocol

When the user reconnects to the AP, as shown in Figure 4, the AP will send a key packet via the EAPOL protocol to the user's device. EAPOL is a type of protocol commonly used for wireless authentication and point-to-point connections. From Figure 4.20, the EAPOL package used is EAPOL-key, which is a package that contains an encryption key or other key that will be used after a successful authentication process. This EAPOL-key packet is captured by the attacker to get the handshake data and perform the password cracking process.

3.4 Report Phase

From the test results obtained, a report is made to determine the security gap in the wireless LAN network

Tabel 2
Report

No	Attack	*Tools*	Information required	Attack Status WPA2-PSK	Attack Status RADIUS Server	Information
1	User penetration authentication					
	Cracking The Encryption	airmon-ng, airodump-ng, aireply-ng, aircrack-ng, wireshark	*Dictionary Word, user handshake, Which channel used and BSSID from access point.*	Success	Failed	Successfully obtained WPA2-PSK acces point password, on access point Unsuccessful because the RADIUS server authentication system uses a captive portal
2	Penetration of the access point					
	Attacking The Infrastructure	DNS-Flood master, wireshark	SSID, access point BSSID, and list of MAC addresses of users connected to the network	Success	Success	Successfully disabled access points
3	Penetration of client data to the access point					
	a. *Bypassing MAC Address*	airmon-ng, airodump-ng, MACChanger, wireshark	List of MAC addresses of users which is connected in network	Success	Success	Successfully connected to the internet using a fake MAC address
	b. *Sniffing* Paket dengan *tools*	Netdiscover, ettercap,	*Ports open on server, IP and*	Success	Success	Successfully obtained user data such as,

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.

No	Attack	*Tools*	Information required	Attack Status WPA2-PSK	Attack Status RADIUS Server	Information
	ettercap	wireshark	*MAC gateway address and user that is connected inward network*			username and password

4. Conclusion

Based on the research that has been carried out during the design to analysis of the security of the Wireless Local Area Network, the following conclusions can be drawn: (i) With the RADIUS server security system that uses captive portal authentication, only registered users can connect to the wireless network. WPA2-PSK is a protocol with flexible security, where the user who wants to connect to the wireless network will be forced to enter a predetermined share key / password. (ii) By carrying out 4 stages of research using the penetration testing method (i) the planning phase, (ii) the discovery phase, (iii) the attack phase and (iv) the report phase). From the attack stage (Cracking The Encryption, Bypassing MAC Address, Attacking The Infrastructure and MITM) using Kali Linux, it gets the results of four types of attacks carried out, only one has failed status, namely the type of cracking the encryption attack on the RADIUS server due to using captive portal authentication . In MAC address Bypassing testing, MAC filtering techniques can be easily tricked, because MAC addresses can be changed virtually using macchanger tools so that if the MAC address registered on the wireless network is known, the attacker will be able to access the wireless network easily. In addition, in testing Attacking The Infrastructure and Man In The Middle, WLAN networks have not been able to provide security to connected users so that do not get interference or wiretaps from attackers when accessing the same internet service.

5. References

[1] Sinambela, J., "Keamanan Wireless LAN (Wifi)", Makalah. Yogyakarta: Universitas Negeri Yogyakarta, 2007
[2] Chow, E, Ethical Hacking dan Penetration Testing, IT Research Paper, Canada: The Centre for Information Integrity and Information Systems Assurance, University, 2011.
[3] https://itgid.org/pengertian-penetration-testing/ (7 Maret 2019)
[4] https://www.guru99.com/learn-penetration-testing.html
[5] Ritzkal. 2020. "Tick Waste Application in Houses With Warning of Microcontroller Assistant Social Media.," Jurnal MANTIK Vol 3, hlm. 559-568.
[6] Ritzkal. 2018. "Manajemen jaringan untuk pemula.," Bogor: UIKA PRESS.
[7] M Subchan, Dedi Setiadi. 2020. "Information System For Sale Of Muslim Clothes Based On E-Commerce Technology.," Jurnal MANTIK Vol 4, hlm. 311-318.
[8] Ritzkal, Arief Goeritno, dan Eko Hadi P, (2017), "Pengukuran Kualitas Perangkat Lunak Sistem E-Learning Menggunakan Metric Function Oriented", Prosiding SNATIF Ke-4 Fakultas Teknik Universitas Muria, Kudus.
[9] Ritzkal, Moh Subchan, (2017), "Pengukuran Kualitas Perangkat Lunak Sistem Manajemen Pelaporan Kegiatan Berbasis Web Peringatan Berbasis Email",Prosiding Seminar Nasional Teknoka ke - 2 UHAMKA, Jakarta.
[10] Ritzkal. 2019. *Keamanan Jaringan Cyber*. Bogor: UIKA Press

Accredited "Rank 4"(Sinta 4), DIKTI, No. 36/E/KPT/2019, December 13th 2019.