WI-FI NETWORK SECURITY ANALYSIS AGAINST PACKET SNIFFING ATTACKSAT PGRI UNIVERSITY WEST SUMATRA

Fatimah*, Thomson Mary[2], Anggri Yulio Pernanda[3]
*Universitas PGRI Sumatera Barat
mmahfati@gmail.com, thomsonmary1980@gmail.com, anggriyulio@gmail.com,

Abstract
The University of PGRI West Sumatra has wi-fi which does not rule out attacks on wi-fi networks carried out by hackers. Network Security is a protector in a network system in the process of preventing unauthorized and irresponsible network users. This research includes descriptive research. Descriptive research method is a research method that aims to explain an event. This research was conducted by testing and analyzing the test results on network security using Wireshark and Ettercap applications (Kali Linux OS). The results of this study in the form of a wi-fi network security system in building A1, building B1, building D1 at University of PGRI West Sumatra is good. During the scan for hosts, the IP of the laptop victim of the packet sniffing attack was not found.
Keywords: Network Security Analysis, Wi-Fi, Packet Sniffing

Abstrak
Universitas PGRI Sumatera Barat memiliki wi-fi yang tidak menutup kemungkinan terjadi serangan pada jaringan wi-fi yang dilakukan oleh hacker. Keamanan Jaringan merupakan suatu pelindung dalam sebuah system jaringan dalam proses untuk mencegah para pengguna jaringan yang tidak berhak dan tidak bertanggung jawab. Penelitian ini termasuk penelitian deskriptif, Metode penelitian deskriptif adalah salah satu metode penelitian yang bertujuan untuk menjelaskan suatu kejadian. Penelitian ini dilakukan dengan cara menguji dan menganalisis hasil pengujian pada keamanan jaringan menggunakan aplikasi Wireshark dan Ettercap (OS Kali Linux). Hasil dari penelitian ini berupa sistem keamanan jaringan wi-fi pada gedung A1, gedung B1, gedung D1 di Universitas PGRI Sumatera Barat sudah baik. Pada saat dilakukan scan for hosts tidak ditemukan IP dari laptop korban penyerangan packet sniffing.
Kata kunci: Analisis Keamanan Jaringan, Wi-Fi, Packet Sniffing

1. INTRODUCTION

Network security is very important to pay attention to, networks connected to the internet are basically insecure and can always be exploited by hackers, both on wired and wireless networks. According to (Hidayat et al., 2018) (Hidayat et al., 2018) Packet Sniffing/Sniffer is an attack method by monitoring all packets that pass through a communication medium, be it cable or wireless media.

PGRI University of West Sumatra has wi-fi which does not rule out the possibility of attacks on the network. Based on interviews conducted at PGRI University, West Sumatra with one of the staff in the ICT room, information was obtained that PGRI University, West

Sumatra distributes cable and wireless network services. The distribution of the wi-fi network in building A, building B, building C, and building D, and also obtained information regarding the security of the wi-fi network at the PGRI University of West Sumatra does not yet know the security of the network.

According to (Suyuti Ma'sum et al., 2017) Network Security is the process of preventing and identifying unauthorized use of a computer network. According to (Dharma & Thamrin, 2020) Wireless Fidelity (Wi-fi) is a technology that allows a number of computers to be connected in a network without cables, aka wireless local area network (WLAN). According to (Iwan Sofana, 2014) a router is a tool used to connect several networks. According to (Fauzi & Suartana, 2018) Packet sniffing is a technique for monitoring every packet that crosses a network, and is a piece of software or hardware that monitors all traffic that crosses a network. According to (Sabdho & Ulfa, 2018) Kali Linux is a Linux distribution system developed with a focus on penetration testing tasks. According to (Putra et al., 2018) Wireshark is a tool intended for analyzing network data packets. According to (Turkhamun Adi Kurniawan, 2020) (Turkhamun Adi Kurniawan, 2020) Ettercap is a tool for network protocol analysis and security auditing.

2. METHOD

Network security is very important to pay attention to, networks connected to the internet are basically insecure and can always be exploited by hackers, both on wired and wireless networks. According to (Hidayat et al., 2018) (Hidayat et al., 2018) Packet Sniffing/Sniffer is an attack method by monitoring all packets that pass through a communication medium, be it cable or wireless media.

PGRI University of West Sumatra has wi-fi which does not rule out the possibility of attacks on the network. Based on interviews conducted at PGRI University, West Sumatra with one of the staff in the ICT room, information was obtained that PGRI University, West Sumatra distributes cable and wireless network services. The distribution of the wi-fi network in building A, building B, building C, and building D, and also obtained information regarding the security of the wi-fi network at the PGRI University of West Sumatra does not yet know the security of the network.

According to (Suyuti Ma'sum et al., 2017) Network Security is the process of preventing and identifying unauthorized use of a computer network. According to (Dharma & Thamrin, 2020) Wireless Fidelity (Wi-fi) is a technology that allows a number of computers to be connected in a wireless network, aka wireless local area network (WLAN). According to (Iwan Sofana, 2014) a router is a tool used to connect several networks. According to (Fauzi & Suartana, 2018) Packet sniffing is a technique for monitoring every packet that crosses a network, and is a piece of software or hardware that monitors all traffic that crosses a network. According to (Sabdho & Ulfa, 2018) Kali Linux is a Linux distribution system developed with a focus on penetration testing tasks. According to (Putra et al., 2018) Wireshark is a tool intended for analyzing network data packets. According to (Turkhamun Adi Kurniawan, 2020) (Turkhamun Adi Kurniawan, 2020) Ettercap is a tool for network protocol analysis and security auditing.

3. FINDINGS AND DISCUSSION

Result

The following are the results of research on the wi-fi network at PGRI University, West Sumatra which was carried out in: Building A1, Building B1, and Building D1.

a. Hotspot in building A1

In Figure below, when testing a packet sniffing attack, the image shows that when the IP of the attack victim's laptop can be detected, we put the IP address of the network on target 1, and the IP address of the attack victim on target 2 in the Ettercap tool

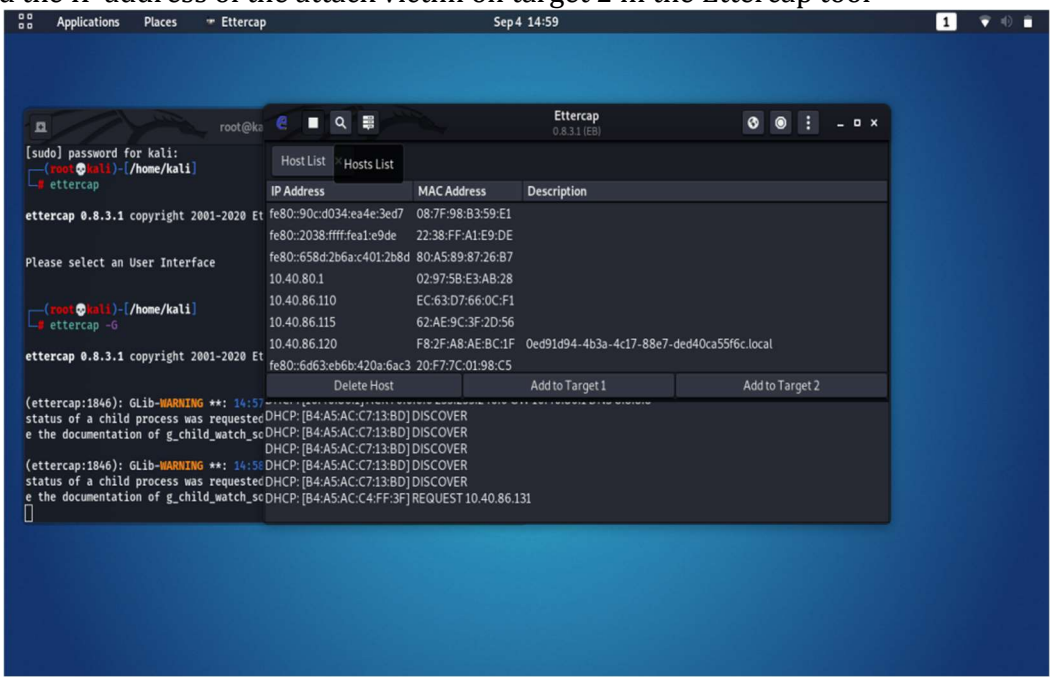


Figure 1. The Ettercap display displays the IP address

In figure below, then open Wireshark, this picture shows the results of doing Capture, when you start pressing "Start capturing packets" on Wireshark it will carry out sniffing according to the configuration that has been done, and the process of capturing data packets that cross a network is will take place in real time. The longer you sniff, the larger the file that will be produced. Laptop 1 as sniffing or attacker

b. Hotspot in building B1

Figure below shows that when testing a packet sniffing attack, the image shows that the IP of the attack victim's laptop was not detected in the Ettercap tool.

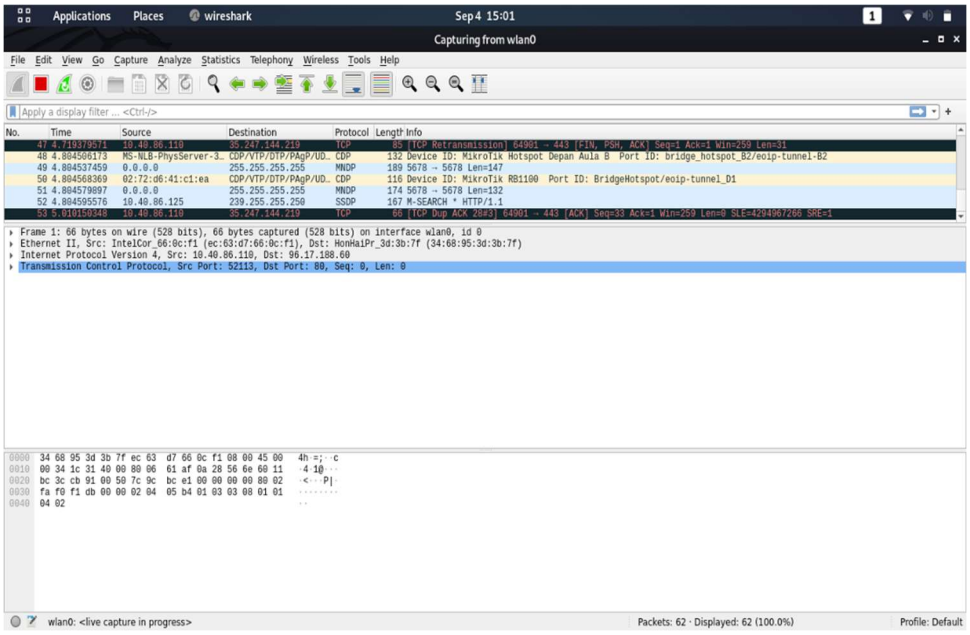


Figure 2. Display When Starting Capture

Figure shows that, when we have started sniffing using Wireshark, laptop 2, as the victim of a sniffing attack, will try to access the sites that will be tested. When trying to access several sites here, it was seen that these sites could not be accessed or reached because automatically on the attack victim's laptop the network access was disconnected and reconnected when sniffing. Because of the hotspot network on A1, the network is very weak, and the network often disconnects and connects, and continuing sniffing cannot be done or stops.

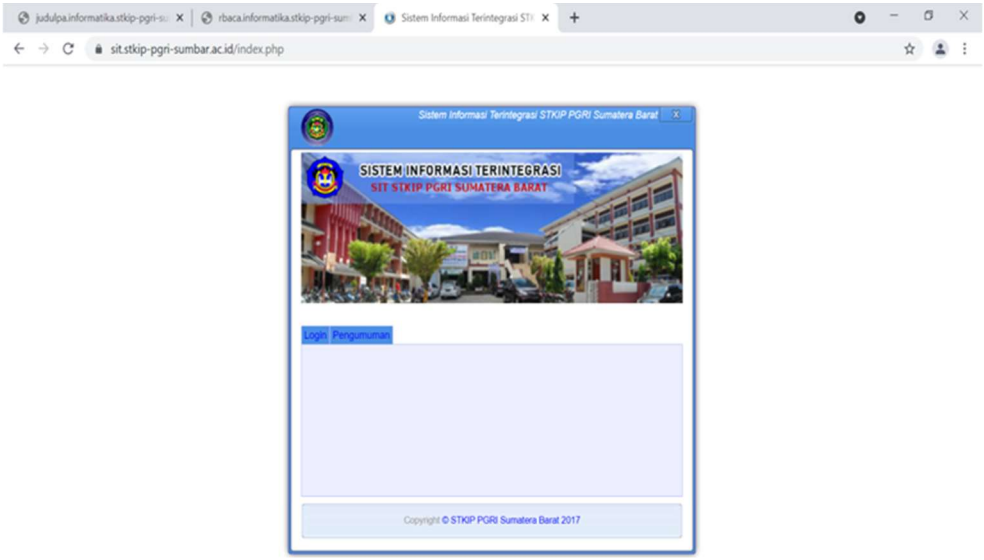


Figure 3. display login

In Figure below, it shows that there is no activity that traverses network traffic from the results captured by the attacker. Here you cannot get data information or access carried

out by the victim of the attack and the activities carried out by the victim of the attack cannot be captured by the attacker. Because while sniffing the Wi-Fi network was disconnected. This research proves that the information data obtained in carrying out packet sniffing attacks on the Wi-Fi network of Building A1 at PGRI University, West Sumatra, especially the hotspot provided for students in Building A1, states that network security is safe.

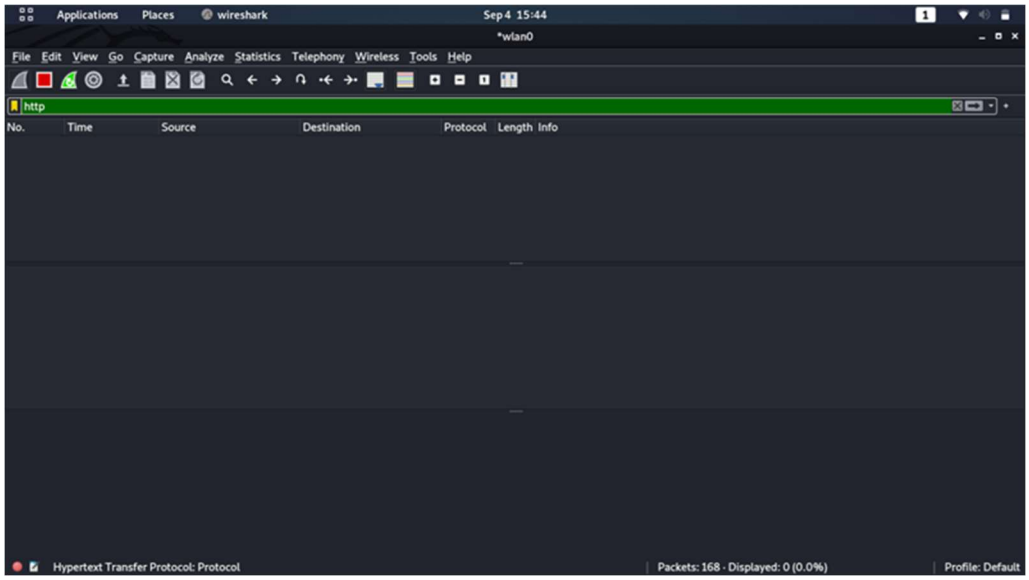


Figure 4. display capture

c. Hotspot in building D1

In the hotspot of building D1, the same as in building B1, the wi-fi network cannot carry out packet sniffing attacks, it is stated that network security is safe.

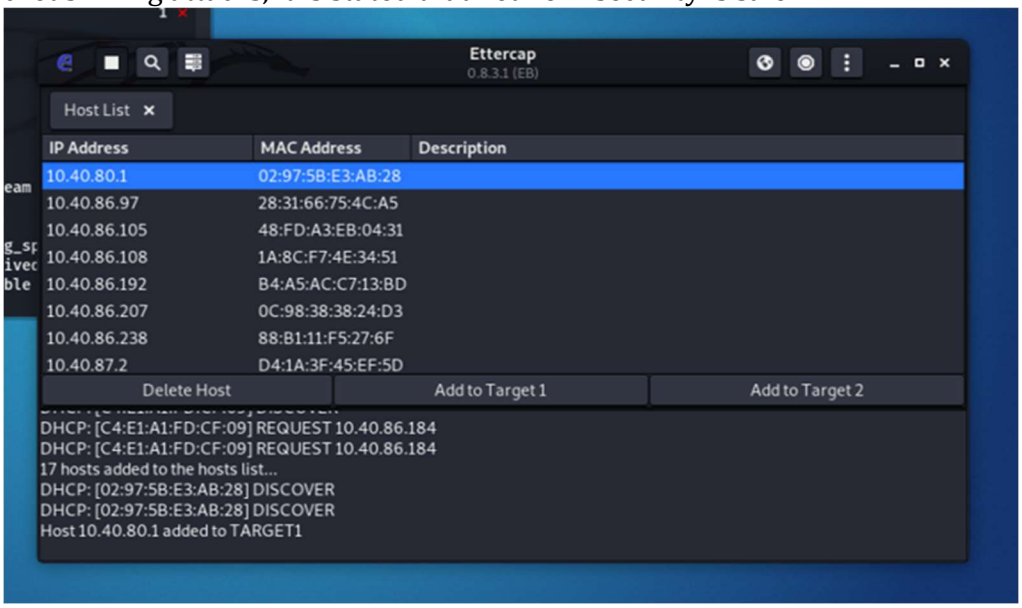


Figure 5. Display Ettercap to show IP address

Figure below shows that when you display Wireshark, the Wireshark application is invalid and cannot be displayed. Automatically sniffing on the hotspot network in building B1 cannot be carried out by packet sniffing attacks. At PGRI University, West Sumatra, it is stated that network security is safe.

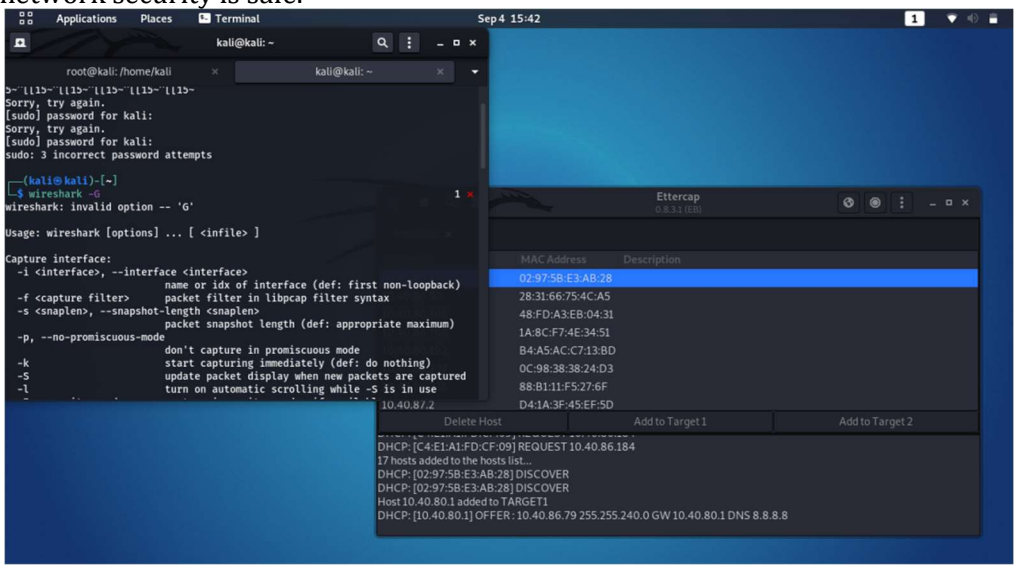


Figure 6. Display when showing wireshark

Discussion

a. Hotspot in building A1

Attempted packet sniffing attacks on wi-fi networks. This was done to determine the level of security of the Wi-Fi network or hotspot provided for PGRI University West Sumatra students. From the results of experiments that have been carried out with 5 services accessing sites, trials using the Wireshark and Ettercap applications on Kali Linux (OS) against packet sniffing attacks, and the results were that no data information was found traversing network traffic when capturing the Wireshark application because the network of the attack victim's laptop was disconnected and connected while sniffing. So, for security, the Wi-Fi network is safe from sniffing attacks that researchers carried out during the research.

b. Hotspot in building B1

Attempted packet sniffing attacks on wi-fi networks. This was done to determine the level of security of the Wi-Fi network or hotspot provided for PGRI University West Sumatra students. From the results of experiments that have been carried out with 5 services accessing sites, trials using the Wireshark and Ettercap applications on (OS) Kali Linux against packet sniffing attacks, and the results when opening the Ettercap tool did not detect the IP address of the attack victim's laptop, so to continue Opening the Wireshark application cannot be done because the IP address of the attack victim cannot be found, and carrying out the sniffing attack cannot be continued. So for security, the Wi-Fi network is safe from sniffing attacks that researchers carried out during the research.

c. Hotspot in building D1

Attempted packet sniffing attacks on wi-fi networks. This was done to determine

the level of security of the Wi-Fi network or hotspot provided for PGRI University West Sumatra students. From the results of experiments that have been carried out with 5 services accessing sites, trials using the Wireshark and Ettercap applications on (OS) Kali Linux against packet sniffing attacks, and the results when opening the Ettercap tool did not detect the IP address of the attack victim's laptop, so to continue Opening the Wireshark application cannot be done because the IP address of the attack victim cannot be found, and carrying out the sniffing attack cannot be continued. So, for security, the Wi-Fi network is safe from sniffing attacks that researchers carried out during the research.

No	Serangan	Titik Pengujian	Situs yang Diuji	Hasil	Keterangan
1	*Packet Sniffing*	*Hotspot* jaringan wi-fi Gedung A1	1. Portal 2. E-learning 3. Sistem TA Pendidikan 4. Sistem Informatika Ruang Baca Pendidikan Informatika Sistem PLK Pendidikan Informatika	Aman	Tidak berhasil menangkap paket data informasi dari jaringan wi-fi untuk mahasiswa
2	*Packet Sniffing*	*Hotspot* jaringan wi-fi Gedung B1	1. Portal 2. E-learning 3. Sistem TA Pendidikan 4. Sistem Informatika Ruang Baca Pendidikan Informatika Sistem PLK Pendidikan Informatika	Aman	Tidak berhasil mendeteksi IP address pada laptop korban terhadap serangan *sniffing* pada jaringan wi-fi untuk mahasiswa
3	*Packet Sniffing*	H*otspot* jaringan wi-fi Gedung D1	1. Portal 2. E-learning 3. Sistem TA Pendidikan 4. Sistem Informatika Ruang Baca Pendidikan	Aman	Tidak berhasil mendeteksi IP address pada laptop korban terhadap serangan *sniffing* pada jaringan wi-fi untuk mahasiswa

			Informatika
	1.	Sistem Pendidikan Informatika	PLK

If you look at the table of research results above, packet sniffing attacks were carried out on Wi-Fi networks or hotspots in building A1, building B1 and building D1 which are specifically for students on the PGRI University West Sumatra campus. When testing, researchers were unable to carry out a Packet Sniffing attack on a Wi-Fi network because the Wi-Fi network at PGRI University, West Sumatra already used network security encryption using WPA2 and the Wi-Fi network at PGRI University, West Sumatra was declared safe from attacks. which has been tested using packet sniffing attacks by researchers. Meanwhile, for the sites being tested, the sites whose data can be captured, namely sites or systems or applications, are those that use the HTTP protocol, while for sites that use the HTTPS protocol the data cannot be obtained, because the data is encrypted or cannot be accessed. be read.

4. CONCLUSION

With an analysis of Wi-Fi network security against packet sniffing attacks at PGRI University, West Sumatra. Cannot detect network security problems because when testing it cannot obtain the IP Address of the testing laptop. Based on the results of data analysis and experiments on packet sniffing attacks that have been carried out, it can be concluded that the Wi-Fi network security system in building A1, building B1, building D1 at PGRI University, West Sumatra is good. The security encryption used at PGRI University of West Sumatra is WPA2 security.

This is proven by the results of research that has been carried out, namely:

1. After testing packet sniffing attacks using the Wireshark and Ettercap applications on (OS) Kali Linux on a Wi-Fi network specifically for students at PGRI University, West Sumatra, absolutely no activity such as accessing site accounts was found.
2. When the packet sniffing attack was carried out, it was discovered that the Wi-Fi network at PGRI University, West Sumatra had been protected with WPA2 security or security encryption.

5. REFERENCES

Dharma, S., & Thamrin, T. (2020). Analisis Kinerja Jaringan WIFI. Voteteknika (Vocational Teknik Elektronika Dan Informatika), 8(2), 35. https://doi.org/10.24036/voteteknika.v8i2.109129

Fauzi, A., & Suartana, I. (2018). Monitoring Jaringan Wireless Terhadap Serangan Packet Sniffing Dengan Menggunakan Ids. Jurnal Manajemen Informatika, 8(2).

Hidayat, M. T., Sn, F. M., & Kurniati, N. I. (2018). Analisis Keamanan Jaringan Pada Fasilitas Internet (Wifi) Gratis Terhadap Serangan Packet Sniffing. 1(2), 112–119.

iwan sofana. (2014). cisco ccna & jaringan komputer. Informatika Bandung.

Putra, E. M., Tujni, B., & Negara, E. S. (2018). Analisis Kemanan Jaringan Internet (Wifi) Dari Serangan Packet Data Sniffing Di Universitas Muhammadiyah Palembang. Jurnal

Ilmiah Teknologi Informasi.

Sabdho, H. D., & Ulfa, M. (2018). Analisis Keamanan Jaringan Wireless Menggunakan Metode Penetration Testing Pada Kantor PT. Mora Telematika Indonesia Regional Palembang. Semhavok, 1(1), 15–24.

Suyuti Ma'sum, M., Azhar Irwansyah, M., & Priyanto, H. (2017). Analisis Perbandingan Sistem Keamanan Jaringan Menggunakan Snort dan Netfilter. Jurnal Sistem Dan Teknologi Informasi (JUSTIN), 5(1), 56–60.

Turkhamun Adi Kurniawan. (2020). ANALISA KEAMANAN JARINGAN WIFI TERHADAP SERANGAN PACKET SNIFFING.