JURNAL TEKNOLOGI DAN OPEN SOURCE
Vol. 8, No. 2, December 2025, pp. 1084~1090
e-ISSN: 2622-1659, accredited Four Grade by Kemenristekdikti, Decree No: 152/E/KPT/2023
DOI: https://doi.org/10.36378/jtos.v8i2.5112

Detection and Analysis of Packet Sniffing Attacks Using Wireshark on Wifi Networks: a Practical Approach to Network Security Case Study of Puskesmas Sungsang

M. Hajaji Alfarizi[1], Zulhipni Reno Saputra Elsi[2], Apriansyah[3], Karnadi[4]
[1,3,4]Department of Information Technology, University of Muhammadiyah Palembang, South Sumatra
[2]Information Technology Study Program, Faculty of Engineering

Article Info

Article history:

Accepted 11 28, 2025
Revision 12 17, 2025
Accepted 12 22, 2025

Keywords:

Packet Sniffing
Wireshark
Network
Phc

ABSTRACT

In the last two decades, advances in internet technology have significantly influenced various sectors, including healthcare. The integration of information technology into health services has become essential for improving operational efficiency through integrated medical information systems, structured patient management, and digital financial administration. The Sungsang Health Center, as a community-based healthcare facility, relies heavily on networked systems to support daily activities such as patient registration and electronic medical record management, which involve highly sensitive data. This condition increases the risk of data leakage, particularly due to packet sniffing attacks. Therefore, strengthening network security policies is a critical need. This research aims to analyze potential packet sniffing threats and support the prevention of data leaks at the Sungsang Health Center by utilizing Wireshark as a network analysis tool. Wireshark enables detailed monitoring and analysis of data packets to identify suspicious activities that are not easily detected manually. The study provides insights into techniques for detecting and analyzing network vulnerabilities, which can serve as a reference for improving network security policies. The results are expected to support the development of safer and more reliable digital health systems and raise awareness of the importance of protecting patient data.

Corresponding authors:

M.Hajaji Alfarizi
Department of Information Technology
University of Muhammadiyah Palembang
South Sumatra, Indonesia
Email: Muhhajaji14@gmail.com

1. Introduction

In the last two decades, advances in internet technology have had a major impact on various aspects of life, including in the health sector. The integration of the internet and information technology is now a vital part of the operations of hospitals, clinics, and health centers[1]. This allows healthcare services to be more efficient through integrated medical information systems, more structured patient management, and faster financial administration. In addition, faster and more affordable internet access has also improved the quality of services, ranging from communication between medical personnel, medical record management, to remote consultation. Indonesia is facing many cases of data leaks due to cyber attacks. IT experts said that one of the reasons was the budget shortfall experienced by the State Cyber and Cryptography Agency. Based on 2022

State Budget data, the budget allocation received by BSSN in 2022 reached IDR 554.6 billion. This budget is down 60% compared to the 2021 outlook of IDR 1.39 trillion[2].

However, this progress also requires special attention to data security, as the risk of leakage of personal and sensitive information is increasing. As the reliance on technology increases, threats to computer network security are becoming more diverse and complex. One example is packet sniffing attacks, where unauthorized parties are able to capture and analyze data packets sent over a network. These attacks are particularly dangerous because they can result in the leakage of important information, such as patients' personal data, medical information, passwords, and transaction data. On Ethernet networks, this type of attack is quite easy to carry out if the network is not equipped with adequate encryption or protection. The basic concept in network security is to maintain the confidentiality, integrity, and availability of data that passes through the network. This principle is known as the CIA triad (*Confidentiality, Integrity, Availability*).

According to Hidayat et al., packet sniffing is an attack method by monitoring all packets passing through a communication medium, both wired and wireless. Therefore, health institutions such as health centers must be aware of the importance of maintaining data security, given the large volume of medical data managed and its vulnerability to attacks. Wireshark is one of the popular and effective network analysis tools in detecting and analyzing packet sniff attacks. The tool allows administrators to capture and examine data packets passing through the network, providing in-depth information about the protocols used and communication patterns between devices. With real-time analytics capabilities, Wireshark can help detect attacks early, enabling quick and precise handling to reduce the risk of data leaks. According to Putra et al., Wireshark is software used for the analysis of network data packets and can help identify potential security threats. Wireshark is a network analysis software that allows users to record and analyze network traffic in real-time. Wireshark can be used to troubleshoot network issues, identify outages, optimize network performance, and even troubleshoot security issues. [3] [4] [5]

Wireshark is one of the most popular and frequently used network analysis tools in the detection of sniffing attacks. Wireshark allows users to capture and examine data that is being transmitted on the network in real-time. With Wireshark, users can view all data packets passing through the network, which includes information about the source, destination, and contents of each packet.

Wireshark can be used in identifying malware, and the research subjects consist of network traffic data captured from high-risk network environments [6]

As an in-depth and comprehensive tool, Wireshark supports a wide range of commonly used network protocols, including TCP/IP, HTTP, HTTPS, and more. Users can perform detailed packet analysis to detect any problems or threats, such as packet sniffing. Wireshark also allows users to filter captured data based on specific criteria, such as IP addresses, protocol types, or even certain suspected keywords.

Data interception on WiFi networks is often done using a sniffing tool, such as Wireshark, which can capture all data packets passing through the network. Typically, the data detected in these attacks is information that is not protected by encryption or uses insecure protocols, such as HTTP. In these conditions, attackers can gain access to various sensitive information, such as credit card numbers, usernames, and passwords used in online communications.

Packet sniffing attacks are particularly effective on networks that don't use adequate encryption, such as public WiFi networks or networks that still use legacy protocols like WEP (Wired Equivalent Privacy). Since the data transmitted on the WiFi network is not protected with strong encryption, all information can be easily accessed by anyone within range of the network. Therefore, the implementation of better security protocols, such as WPA2 or WPA3, is essential to protect data from snifting attacks.

Packet sniffing is not only dangerous in the context of retrieving personal information, but it can also be used by attackers to analyze larger communication patterns within a network. For example, in the context of health centers, an attacker who is able to access communication data between medical devices or administrative systems can reveal sensitive information about patients or internal operations, which can compromise patient privacy.

To prevent sniff attacks, there are several measures that can be implemented, such as the use of end-to-end data encryption, VPNs, and network access restrictions. On the other hand, it is also important for network administrators to regularly monitor network traffic to detect suspicious activity that may indicate unauthorized conversations or data transfers. Therefore, an understanding of how sniffing attacks work and techniques for identifying them is essential for healthcare providers such as health centers.

The Sungsang Health Center, as one of the health facilities that serves the community, relies heavily on information systems to support daily operations. Networks that connect various devices, from patient registration systems to electronic medical record management, store highly sensitive data. The risk of data leakage due to packet sniffing attacks, if not detected, can have a negative impact on patients and the institution itself. Therefore, the use of tools such as Wireshark is crucial to detect and identify potential attacks to maintain data security and privacy. Through analysis with Wireshark, patterns or indications of attacks can be identified so that appropriate mitigation measures can be implemented immediately[7].

With a deep understanding of how packet sniffing attacks work and the use of Wireshark to analyze them, it is hoped that the Sungsang Health Center can strengthen their network security policies and prevent data leaks. It also provides a clear overview of analysis techniques that are able to detect threats that may not be visible to the naked eye, so that data security can be more guaranteed. In addition, this research is expected to increase awareness of the importance of network security in the health sector. With the increasing sophistication of network technology, cyberattacks targeting sensitive data are becoming a serious threat. It is important for health centers to have a strong defense system to protect medical data.

This study seeks to provide in-depth insights into how Wireshark can be used to identify, analyze, and prevent packet sniffing attacks that have the potential to damage the reputation and integrity of patient data. The results of the research can later be used as a reference for the Sungsang Health Center in developing better and more effective network security policies, as well as providing insight to other health institutions about the importance of protecting sensitive data. In the future, this research is also expected to be the basis for the development of more sophisticated cyberattack detection technologies and procedures in creating a safer digital health ecosystem.

2. Research Methods

2.1 Research Approach

This study uses an experimental method with a practical approach to analyze packet sniffing attacks on WiFi networks using Wireshark. The experiment was carried out by capturing and analyzing data packets passing through the WiFi network to detect potential security threats. With this method, it is hoped that the extent of data communication security on the WiFi network can be known, especially in the face of potential sniff attacks.

Packet sniffing is a technique used to analyze data traffic sent over a computer network. This technique allows a third party to capture data packets transmitted between two devices, such as computers and servers. In a sniffing attack, an attacker attempts to monitor and access unprotected information, such as login credentials, personal data, or other sensitive information sent over the network.

The approach used in this study includes observing network traffic, collecting data on packets passing through the network, and analysis of packets that are indicated as security threats. This technique allows the identification of communication patterns in the WiFi network used, both under normal conditions and under conditions at risk of attack.

This research was conducted in a controlled environment to ensure the validity of the results. The WiFi network used has obtained access permissions, so it does not violate the ethical aspects of cybersecurity research. In addition, the use of Wireshark. Wireshark is a network analysis software that allows users to record and analyze network traffic in real-time. Wireshark can be used to troubleshoot network issues, identify outages, optimize network performance, and even troubleshoot security issues. [8]

Wireshark is one of the most popular and frequently used network analysis tools in the detection of sniffing attacks. Wireshark allows users to capture and examine data that is being transmitted on the network in real-time. With Wireshark, users can view all data packets passing through the network, which includes information about the source, destination, and contents of each packet.

Wireshark can be used in identifying malware, and the research subjects consist of network traffic data captured from high-risk network environments [9]

As an in-depth and comprehensive tool, Wireshark supports a wide range of commonly used network protocols, including TCP/IP, HTTP, HTTPS, and more. Users can perform detailed packet analysis to detect any problems or threats, such as packet sniffing. Wireshark also allows users to filter captured data based on specific criteria, such as IP addresses, protocol types, or even certain suspected keywords. As a key tool in this study it allows testing various aspects of network traffic, including data encryption and potential eavesdropping.

The tools and materials used in this study include:

1. Software:
   a) Wireshark latest version
   b) Windows/Linux operating system with monitor mode support
2. Hardware:
   a) Laptops with network cards that support monitor mode
   b) Active WiFi network (with access permissions)
   c) Router WiFi
3. Trial Website:

a) https://banyuasin.epuskesmas.id (as the target of HTTPS data traffic)

Wireshark was chosen for its ability to capture and analyze network packets in real-time. In addition, the protocols observed in this study are DNS, TLS, and HTTP, which can provide information about the security of the network being tested. With the appropriate combination of software and hardware, the study can provide valid and relevant results.

Tools and Materials

2.2 Research Procedure

1. Preparation

1) Wireshark installation and hardware configuration that supports monitor mode.
2) Testing the connection to the WiFi network to be observed.
3) Ensures that the device can capture packets passing over the WiFi network.

2.3 Data Collection

1) Run Wireshark and select the WiFi network interface.
2) Enable packet filters based on specific protocols such as DNS, TLS, and HTTP.
3) Observe the communication between the client and the server while accessing the banyuasin.epuskesmas.id.
4) Take a screenshot of the package capture for documentation.

2.4 Data Analysis

One of the main advantages of Wireshark is its ability to understand and display the structure of various network protocols. Wireshark can parsing and display fields in packets according to the protocol specifications used, such as TCP/IP, UDP, HTTP, and many others. This allows users to view the details of each packet, including headers and payloads, as well as analyze the behavior of the protocol in network communications.

1) Identify captured data packets, including analysis of TLS packets.
2) Analyzes DNS packets to detect possible manipulation or spoofing.
3) Detects possible Man-in-the-Middle (MITM) attacks or other anomalous packets.
4) Compare normal traffic with traffic indicated to be intercepted.

3. Results and Discussion

This experiment aims to identify potential security threats to WiFi networks by using Wireshark. In this experiment, data packets were captured on WiFi networks that accessed banyuasin.epuskesmas.id. The packet capture is analyzed to see how the communication between the client and the server is going, as well as the extent of its security in the face of a eavesdropping attack.

Computer network security is a series of efforts made to protect the data, hardware, and software in a computer network from threats that can threaten its integrity and confidentiality. Network security is a crucial foundation in facing the rapid development of technology today. In an era where digital connectivity is becoming more and more profound, network security is becoming a key pillar to protect sensitive data, prevent cyberattacks, and ensure system integrity [9].

The basic concept in network security is to maintain the confidentiality, integrity, and availability of data that passes through the network. This principle is known as the CIA triad (*Confidentiality, Integrity, Availability*).

Confidentiality means that data should only be accessed by authorized parties, while integrity ensures that the data sent or received is not subject to unauthorized alteration. Availability refers to the ability of the system to continue to provide services to legitimate users without interruption, even when faced with attacks or damage. These three principles are the cornerstones of all network security strategies and policies.

As information technology develops, threats to computer networks are also increasingly diverse. Internal threats and *external* threats can come from a variety of sources, both intentional and unintentional. External threats are usually attacks from outside the network that do not have permission to access the system, such as *hackers* or *crackers*. On the other hand, *internal threats* often come from employees or individuals who have legitimate access, but use that access for detrimental purposes.

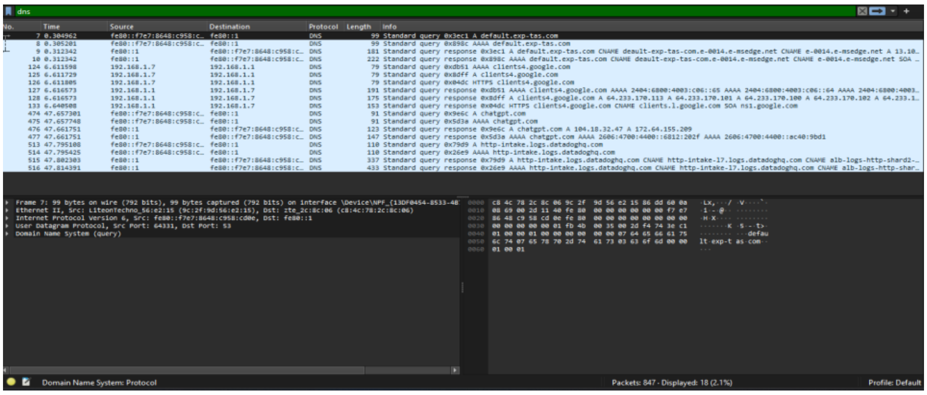
One method used to maintain network security is authentication, which aims to ensure that only legitimate users can access network resources. Authentication can be done in a variety of ways, from the use of passwords to two-factor authentication (2FA). In addition, *encryption* is important to protect data transmitted over the network from being accessed by unauthorized parties. Encryption technologies such as SSL/TLS are used to secure data in the transmission process

By capturing network traffic, this study aims to find out whether sensitive data such as usernames and passwords can be exposed in the network. In addition, DNS, TLS, and HTTP packets are analyzed to see if there is a possibility of data manipulation or attacks such as Man-in-the-Middle (MITM) and DNS Spoofing. The results of this experiment will provide insights into the effectiveness of encryption in protecting user data as well as provide recommendations to improve network security.

3.1 Package Capture Results

The experiment was conducted by running Wireshark on a WiFi network and capturing packet traffic when accessing banyuasin.epuskesmas.id. From the catches, several interesting network traffic patterns were found to be analyzed. Some of the key findings are:

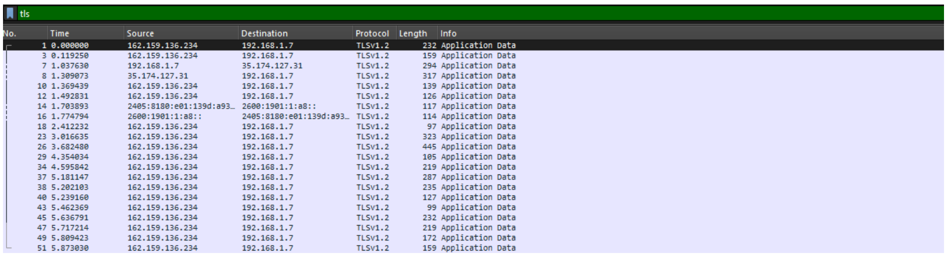
a) DNS packets that indicate access requests to a website domain



```
dns
No.   Time       Source                    Destination               Protocol Length Info
    7 0.304962   fe80::f7e7:8648:c958:c…   fe80::1                   DNS         99 Standard query 0x3ec1 A default.exp-tas.com
    8 0.305201   fe80::f7e7:8648:c958:c…   fe80::1                   DNS         99 Standard query 0x898c AAAA default.exp-tas.com
    9 0.312342   fe80::1                   fe80::f7e7:8648:c958:c…   DNS        181 Standard query response 0x3ec1 A default.exp-tas.com CNAME deault-exp-tas-com.e-0014.e-msedge.net CNAME e-0014.e-msedge.net A 13.10…
   10 0.312342   fe80::1                   fe80::f7e7:8648:c958:c…   DNS        222 Standard query response 0x898c AAAA default.exp-tas.com CNAME deault-exp-tas-com.e-0014.e-msedge.net CNAME e-0014.e-msedge.net SOA …
  124 6.611598   192.168.1.7               192.168.1.1               DNS         79 Standard query 0xdb51 AAAA clients4.google.com
  125 6.611729   192.168.1.7               192.168.1.1               DNS         79 Standard query 0x8dff A clients4.google.com
  126 6.611805   192.168.1.7               192.168.1.1               DNS         79 Standard query 0x04dc HTTPS clients4.google.com
  127 6.616573   192.168.1.1               192.168.1.7               DNS        191 Standard query response 0xdb51 AAAA clients4.google.com AAAA 2404:6800:4003:c06::65 AAAA 2404:6800:4003:c06::64 AAAA 2404:6800:4003…
  128 6.616573   192.168.1.1               192.168.1.7               DNS        175 Standard query response 0x8dff A clients4.google.com A 64.233.170.113 A 64.233.170.101 A 64.233.170.100 A 64.233.170.102 A 64.233.1…
  133 6.640508   192.168.1.1               192.168.1.7               DNS        153 Standard query response 0x04dc HTTPS clients4.google.com CNAME clients.l.google.com SOA ns1.google.com
  474 47.657301  fe80::f7e7:8648:c958:c…   fe80::1                   DNS         91 Standard query 0x9e6c A chatgpt.com
  475 47.657748  fe80::f7e7:8648:c958:c…   fe80::1                   DNS         91 Standard query 0x5d3a AAAA chatgpt.com
  476 47.661751  fe80::1                   fe80::f7e7:8648:c958:c…   DNS        123 Standard query response 0x9e6c A chatgpt.com A 104.18.32.47 A 172.64.155.209
  477 47.661751  fe80::1                   fe80::f7e7:8648:c958:c…   DNS        147 Standard query response 0x5d3a AAAA chatgpt.com AAAA 2606:4700:4400::6812:202f AAAA 2606:4700:4400::ac40:9bd1
  513 47.795108  fe80::f7e7:8648:c958:c…   fe80::1                   DNS        110 Standard query 0x79d9 A http-intake.logs.datadoghq.com
  514 47.795425  fe80::f7e7:8648:c958:c…   fe80::1                   DNS        110 Standard query 0x26e9 AAAA http-intake.logs.datadoghq.com
  515 47.802303  fe80::1                   fe80::f7e7:8648:c958:c…   DNS        337 Standard query response 0x79d9 A http-intake.logs.datadoghq.com CNAME http-intake-17.logs.datadoghq.com CNAME alb-logs-http-shard2-…
  516 47.814391  fe80::1                   fe80::f7e7:8648:c958:c…   DNS        433 Standard query response 0x26e9 AAAA http-intake.logs.datadoghq.com CNAME http-intake-17.logs.datadoghq.com CNAME alb-logs-http-shar…

> Frame 7: 99 bytes on wire (792 bits), 99 bytes captured (792 bits) on interface \Device\NPF_{13DF0454-8533-4B
> Ethernet II, Src: LiteonTechno_56:e2:15 (9c:2f:9d:56:e2:15), Dst: zte_2c:8c:06 (c8:4c:78:2c:8c:06)
> Internet Protocol Version 6, Src: fe80::f7e7:8648:c958:cd0e, Dst: fe80::1
> User Datagram Protocol, Src Port: 64331, Dst Port: 53
> Domain Name System (query)

0000  c8 4c 78 2c 8c 06 9c 2f  9d 56 e2 15 86 dd 60 0a   ·Lx,···/ ·V····`·
0010  08 69 00 2d 11 40 fe 80  00 00 00 00 00 00 f7 e7   ·i·-·@·· ········
0020  86 48 c9 58 cd 0e fe 80  00 00 00 00 00 00 00 00   ·H·X···· ········
0030  00 00 00 00 00 01 fb 4b  00 35 00 2d f4 74 3e c1   ·······K ·5·-·t>·
0040  01 00 00 01 00 00 00 00  00 00 07 64 65 66 61 75   ········ ···defau
0050  6c 74 07 65 78 70 2d 74  61 73 03 63 6f 6d 00 00   lt·exp-t as·com··
0060  01 00 01                                           ···

Domain Name System: Protocol          Packets: 847 · Displayed: 18 (2.1%)          Profile: Default
```

Picture 1. DNS Query Results

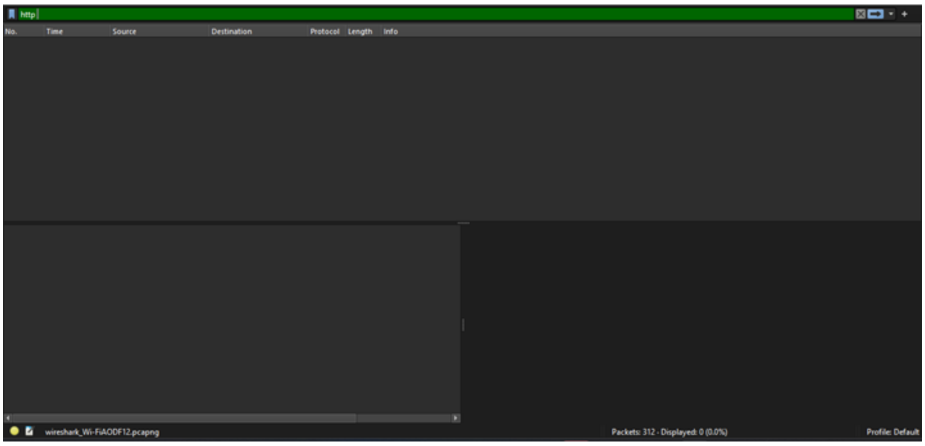
b) A handshake TLS packet that indicates the process of encrypting the communication.



```
tls
No.  Time       Source                    Destination               Protocol Length Info
   1 0.000000   162.159.136.234           192.168.1.7               TLSv1.2     232 Application Data
   3 0.119250   162.159.136.234           192.168.1.7               TLSv1.2     159 Application Data
   7 1.037630   192.168.1.7               35.174.127.31             TLSv1.2     294 Application Data
   8 1.309073   35.174.127.31             192.168.1.7               TLSv1.2     317 Application Data
  10 1.369439   162.159.136.234           192.168.1.7               TLSv1.2     139 Application Data
  12 1.492831   162.159.136.234           192.168.1.7               TLSv1.2     126 Application Data
  14 1.703893   2405:8180:e01:139d:a93…   2600:1901:1:a8::          TLSv1.2     117 Application Data
  16 1.774794   2600:1901:1:a8::          2405:8180:e01:139d:a93…   TLSv1.2     114 Application Data
  18 2.412232   162.159.136.234           192.168.1.7               TLSv1.2      97 Application Data
  23 3.016635   162.159.136.234           192.168.1.7               TLSv1.2     323 Application Data
  26 3.682480   162.159.136.234           192.168.1.7               TLSv1.2     445 Application Data
  29 4.354034   162.159.136.234           192.168.1.7               TLSv1.2     105 Application Data
  34 4.595842   162.159.136.234           192.168.1.7               TLSv1.2     219 Application Data
  37 5.181147   162.159.136.234           192.168.1.7               TLSv1.2     287 Application Data
  38 5.202103   162.159.136.234           192.168.1.7               TLSv1.2     235 Application Data
  40 5.239160   162.159.136.234           192.168.1.7               TLSv1.2     127 Application Data
  43 5.462369   162.159.136.234           192.168.1.7               TLSv1.2      99 Application Data
  45 5.636791   162.159.136.234           192.168.1.7               TLSv1.2     232 Application Data
  47 5.717214   162.159.136.234           192.168.1.7               TLSv1.2     219 Application Data
  49 5.809423   162.159.136.234           192.168.1.7               TLSv1.2     172 Application Data
  51 5.873030   162.159.136.234           192.168.1.7               TLSv1.2     159 Application Data
```

Picture 2. TLS Results

c) No HTTP packets with plaintext username/password were found, because the website uses HTTPS.



```
http
No.  Time  Source  Destination  Protocol  Length  Info

wireshark_Wi-FiAODF12.pcapng          Packets: 312 · Displayed: 0 (0.0%)          Profile: Default
```

Picture 3 Http Package Results

A screenshot of a handshake TLS packet on Wireshark shows that the communication between the client and the server uses strong encryption. This signifies that the data being sent, including login credentials, is protected from packet sniffing attacks.

3.2 Security Analysis

The results of the analysis showed that the communication between the client and the server was well encrypted using the TLS protocol, so sensitive data such as usernames and passwords could not be sniffed directly through Wireshark. This protocol ensures that even if data packets are captured, their contents cannot be read without the appropriate encryption key.

However, some of the potential threats detected are:

1. DNS Spoofing If there is a DNS packet directed to a suspicious IP, this could be a sign of an attack.
2. MITM Attack If there is a TLS packet that shows a discrepancy in the server's certificate, this could be an indication of a data eavesdropping attack.

To ensure that communications are secure, it is necessary to check the stolen SSL/TLS certificate by the website. If there is a change in the accepted certificate compared to what it should be, then there is a possibility of a Man-in-the-Middle attack

3.3 Discussion

From the results of the experiment, it can be concluded that HTTPS is effective in protecting user data from packet sniff attacks. However, other methods such as MITM Attack and DNS Spoofing can still be used to steal information if users are not careful. This suggests that encryption alone is not enough to fully protect user data without additional security measures.

To improve network security, it is recommended:

1. Use a VPN to prevent MITM attacks.
2. Implement DNS Security Extensions (DNSSEC) to be more secure from DNS Spoofing.
3. Ensure that the HTTPS certificates used are genuine and not modified by third parties.
4. Use firewalls and intrusion detection systems (IDS) to monitor suspicious traffic on the network.

By taking these precautions, the risk of data eavesdropping can be significantly reduced. In addition, users of WiFi networks should also always be aware of unknown connections and avoid public networks that do not have an adequate level of security.

4. Conclusion

Usernames and passwords cannot be retrieved directly by the attacker. However, threats such as Man-in-the-Middle (MITM) attacks and DNS spoofing can still occur if users are not careful in choosing a network or if the network they are using does not have adequate protection. In addition, this study also proves that Wireshark is a very effective tool in detecting network traffic and identifying potential security threats that can occur in data communication on WiFi networks.

Suggestion

To improve network security from packet sniffing threats, some of the recommended steps are as follows. First, users should use a VPN to encrypt internet traffic, especially when using public WiFi networks to make data communication safer from eavesdropping. Second, enabling DNSSEC can help protect against DNS spoofing attacks that can redirect users to malicious fake websites. Third, it is crucial for users to always verify HTTPS certificates before entering sensitive information to ensure that there is no manipulation in communication between clients and servers. Fourth, users should avoid public WiFi networks that don't have strong encryption, as these networks are more vulnerable to data eavesdropping attacks. Finally, regular network traffic monitoring is also necessary to detect suspicious activity that could indicate a security attack. By implementing these measures, it is hoped that network security can be improved and the risk of packet sniffing attacks can be minimized.

Reference

[1] Alsharabi, et al. (2023). Detect unusual activity on local networks using Snort and Wireshark tools. Journal of Information Technology Advancement, 14 (4),, 616-624.

[2] Arini, et al. (2023). Wi-Fi Network Security Against Packet Sniffing Attacks Using Firewall Rule (Case Study :Pt.Akurat.Co). Cybersecurity and Digital Forensics E-ISSN: 2615-8442Vol. 6, No. 2, November 2023, pp. 30-38, 30-38.

[3] Cahyawati, et al. (2023). Network Security Design Using the Firewall Security Port Method. In Proceedings of the Amikom Surakarta National Seminar, 203-209.

[4] Cahyawati, R. K. (2023). Network Security Design Using the Firewall Security Port Method. NATIONAL SEMINAR AMIKOM SURAKARTA (SEMNASA) 2023.

[5] D. Wicaksono, ". (2022). Network Security System Firewall Using Firewall with Port Blocking and Firewall Filtering Methods. JATISI (Tek Journal. Inform. Then Sist. Information), vol. 9, no. 2, pp. 1380–1392, 2022, doi: 10.35957/jatisi.V9i2.2103, 1380-1392.

[6] Darmawan, M. A. (2024). NETWORK SECURITY ANALYSIS AGAINST SNIFFING USING WIRESHARK. Just IT : Journal of Information Systems, Information Technology and Computers.

[7] F. N. E. M. , & Sons. (2018). Internet Network Security (Wi-Fi) Analysis of Packet Data Sniffing Attack at the University of Muhammadiyah Palembang. Scientific Journal of Information Technology, 2018.

[8] F. N. Hidayat, et al. (2018). Network security analysis on Internet facilities (Wi-Fi) is free against packet sniffing attacks. Journal of Information Technology, Vol. 1, No. 2, 112-119.

[9] F. N. N. I. Kurniati, ". (2018). Network Security Analysis on Free Internet Facilities (Wi-Fi) Against Packet Sniffing Attacks. Journal of Information Technology, Vol. 1, No. 2, 112–119.

[10] Fauzi, et al. (2018). Wireless network monitoring against packet sniffing attacks using ids. J. Manaj. Inform, 8(2), 7.

[11] Hartomo, K. D. (2007). ANALYSIS OF THE DESIGN OF INTRUSION DETECTION SYSTEM (IDS) SOFTWARE ON COMPUTER NETWORKS BASED ON MOBILE TECHNOLOGY. National Seminar on Systems and Informatics 2007; Bali.

[12] Jain, G. (2021). Applications of Snort and Wireshark in network traffic analysis. In IOP Conference Series: Materials Science And Engineering (Vol. 1119, No. 1, P. 012007) IOP Publishing.

[13] Luthfansa, & et al. (2021). The use of wireshark to sniffing data communication with the HTTP protocol on the internet network. Journal of Information Engineering And Educational Technology) ISSN, 2549, 869X.

[14] Luthfansa, Z. M., & Rosiani, U. D. (2021). The use of wireshark to sniffing data communication with the HTTP protocol on the internet network. Journal of Information Engineering And Educational Technology) ISSN, 2549, 869X.

[15] Mabsali, et al. (2022). The effectiveness of the Wireshark tool for detecting attacks and vulnerabilities in network traffic. in the 1st International Conference on Innovation in Information Technology and Business (ICIITB).

[16] Mulyanto, et al. (2024). Computer network security analysis uses intrusion detection system (IDS) and firewall methods. Digital Transformation Technology.

[17] N. M. M. Listyawati, & Et al. (2022). Implementation and analysis of system profiles on Paloalto Firewall virtualization based on compute resource metrics,". Journal of Computer and Information Systems Vol. 4, No.1.

[18] N. Tamsir. (2023). Information System Security. Bandung: Indie Press.

[19] Novita, et al. (2021). Wifi Security Analysis Using Wireshark. JES (Journal of Electro Smart), 1(1), 1–3, 1-3.

[20] O. Rivaldi, & N. L. Marpaung, ". (2023). The Implementation of Network Security Systems Using the Suricata-Based Intrusion Prevention System,. " INOVTEK Polbeng -Seri Inform., Vol. 8, No. 1, 141.

[21] Scott, N. F. (2025). Analysis of the Implementation of the Electronic-Based Government System (SPBE) in Improving the Efficiency of Public Services in Indonesia. Digital Footprint. Multidisciplinary Scientific Journal.

[22] Putra, et al. (2018). The implementation of a network security system using a VPN with the PPTP method at Pt. Asri Pancawarna. IJCIT (Indonesian Journal On Computer And Information Technology), 3(2).

[23] Sugiyono. (2017). Quantitative, Qualitative and R&D Research Methods. Bandung: Alvabeta.

[24] Suherdi, D. (2021). The use of firewalls on the network uses the RB951Ui–2hnd microtik. Journal of Information Systems Technology and TGD Computer Systems, 4(2).

[25] Yuazijah, A., & et al. (2024). THE NETWORK MONITORING SYSTEM USES THE QUALITY OF SERVICE (Qos) METHOD WITH THE DUDE SOFTWARE (CASE STUDY: PT. ATLAS LINTAS INDONESIA). JATI (Journal of Informatics Engineering Students), 12137-12142.