International Journal of Multidisciplinary Research and Growth Evaluation

International Journal of Multidisciplinary Research and Growth Evaluation
ISSN: 2582-7138
Received: 07-12-2020; Accepted: 10-01-2021
www.allmultidisciplinaryjournal.com
Volume 2; Issue 1; January-February 2021; Page No. 79-82

Wireshark Packet Capture: The technology accounting information system perspective

Lidia Febrika Panjaitan[1], Fransisca Desliana Sinukaban[2], Iskandar Muda[3]
[1, 2, 3] Universitas Sumatera Utara, Medan, Indonesia

Corresponding Author: **Lidia Febrika Panjaitan**

Abstract

The development of information technology is very rapid and gives a positive look to the success of the entity in various business fields. This journal explains how an entity can manage network usage in order to provide maximum benefits for its business through wireshark and identify data leaks. Wireshark is a network analyzer program with the most complete a Graphical User Interface (GUI) display for now. Wireshark is not a tool for hacking, but because it can read everything, it is often used to snoop on sensitive data that is not encrypted. This function can actually secure the entity from hackers if it is properly used. This journal uses the literature study method in its research by examining the previous literature to describe in more detail about wiresharks in the perspective of accounting information technology system. Because the results show that the use of the network besides having advantages there are also disadvantages, especially in the security issue of an entity's important information, but this problem can be minimized by using wireshark, namely by early identification of data leaks.

Keywords: Network, Wireshark, Accounting Information System

1. Introduction

The development of information technology, of course, provides many conveniences in all aspects of life including the business world. One of the benefits that information technology offers is acceleration and accuracy, which in turn will influence decisions based on the information presented. However, besides the many positive benefits, technology also has the disadvantages of data or information leaks. For that we need a quick response based on early identification using a wireshark.

Wireshark is a network analyzer that allows us to see what's happening on the network. This allows us to dissect network packets at a microscopic level, providing in-depth information about individual packets. Wireshark is one of the most popular network analysis programs today, but oddly enough, this program is mostly known not for its main function but because it is often used for beginner hacking purposes. Because there is a deflection of this function, it is very interesting to discuss the function and meaning of wireshark and how to use wireshark.

The Wireshark application itself is one of the Network Analyzer tools or often referred to as a complete network protocol analyzer. Commonly used by Network Administrators network problem solving, software analysis, communication protocol development and education. This program can record all passing packages and select and display the data in as much detail as possible, for example posting comments on blogs or even Username and Password.

Some of the Wireshark capture results include Frame, Ethernet, Internet Protocol, User-Datagram Protocol, Link-local Multicast Name Resolution. The app was originally called Ethereal, and in May 2006 the project was renamed WIreshark due to trademark issues.

The programming language used is the C language with the GNU general public license. Wireshark is widely preferred because of its interface that uses a Graphical User Interface (GUI) or a graphical display.

The outline of how a wireshark works consists of two stages, namely (1.) Record all packets that pass through the selected interface (Interface is a connecting device between networks, can be via wifi or ethernet / lan card, (2.) The results of the recording can be analyzed. Here we can filter what protocol we want such as tcp, http, udp and so on. Wireshark can also record cookies, posts and requests.

2. Literature Review

2.1. Network

A data communication network or computer network is a group of computers that are connected to each other using certain protocols and transmission media.

Based on the coverage area achieved by computer networks, it can be classified into: Local Area Network (LAN) and Wide area Network (WAN).

LAN coverage area smaller than WAN usually consists of a group of buildings that are close together. Actually there are two types of connections that are usually used, the first is a connection that uses a wireless method and the second is a connection that uses a fiberoptic cable. For example, the network contained in the Bank. Of course, every bank has a head office and branch offices. From each office, be it the head office or branch, of course, has a LAN (Local Area Network) where the merger of the existing LAN networks in each office will form a MAN network. This MAN network can usually support both text and voice data. It can even be associated with radio waves or cable television networks. Wireless MAN can usually play on several frequencies, including 900 MHz, 1.5 GHz, 2 GHz, 2.5 GHz, 3.3 GHz, and 5.8 Ghz. And the frequency currently permitted by the Government of Indonesia for use by the general public is at the 2.4 GHz frequency. The function of the MAN network itself is to build and implement a network system that combines servers with the aim of being able to meet all the internal needs of companies and government in communicating a network that is used so that it can carry out various activities such as chat, messenger, and others using local bandwidth.

WAN (Wide Area Network) is a network used to make interconnections between local computer networks that are not physically close to each other, which can be physically separated from cities, provinces or even across geographic boundaries - across countries and continents.

2.2. Literature Interface

User Interface is a visual display of a product that bridges the system with the user (user).

The user interface can be in the form of shapes, colors, and text which are designed to be as attractive as possible. In simple terms, the user interface is how a product is viewed by the user. This user interface is applied to operating systems, applications, websites and blogs. The user interface is designed with several design aspects, starting from the layout, logo images, choosing appropriate colors, easy-to-read typography and other things to enhance your appearance. Applications, websites, or blogs that don't have a good user interface. Users can immediately leave the product before seeing the full contents.

User interfaces with good character will bring benefits to the user entity, including facilitating user interaction with products, increasing sales and business growth and increasing the branding quality of a product / service.

To enjoy the benefits of a user interface, the user interface must be designed to be clear, concise but attractive. Responsive design will make users feel comfortable visiting, in addition to the design required structured, intuitive, consistent information structure and color contrast that is friendly to the user's eyes.

User interfaces are very important, especially for digital products, whether applications, websites or blogs. User interface owners need to pay attention to the appearance of the product user interface to succeed the product goals.

A good user interface is predicted as one of the steps to increase sales and business growth. In addition, a good user interface can be used as an online store branding.

2.3 Wireshark

The main Wireshark application functions are quite a lot. However, strangely this program is mostly known not for its main function but because it is often used for beginner hacking purposes.

Actually wireshark is not designed for hacking / hackers. The main function of the Wireshark application is not intended for hacking. The main function of the Wireshark application is as a Network Administrator to be able to track what is happening in his network or to make sure the network is working properly, and no one does bad things on the network. The main function of the Wireshark application is used to perform network analysis and troubleshooter. This makes it possible to find out what problems occur on the network. Wireshark is a network analyzer program that is very popular today.

Here are some functions of the Wireshark application that you need to know:

1. The main function of the Wireshark application is used by network administrators to analyze network performance. Wireshark is able to capture data packets or information traveling in the visible network. All types of information can be easily analyzed, namely by using sniffing, by sniffing important information such as passwords for other accounts.
2. The Wireshark application function is very useful for network professionals, network administrators, researchers, to network software developers. This is because Wireshark is a software for analyzing computer network traffic,
3. Wireshark application function can analyze data packet transmission in the network, process
4. connection and data transmission between computers. The Wireshark application function can also read data directly from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, and ATM connections.
5. The function of the Wireshark application is also often used by chatters to find out the ip of the victim and other chatter via typing room.

As long as you can get packets directly from the network, with tools like wireshark, you can use wireshark to "tap" Voice over IP conversations.

Wireshark is useful for network administrators even against Hackers as follows:

1. Loopback network, in a wirehark you can find an unreasonable number of packets due to network loops, for example, suddenly there are thousands of packets in seconds.
2. Detect problematic http packets (usually not reaching the server) by looking at the black packet.
3. Malware that continuously sends data, in this case we can see an IP ip that feels foreign, for example during rest hours and no one is accessing the computer but it turns out that the computer shows that the computer is sending data to a suspicious address.
4. WireShark can also see activities such as copying files that have been shared by other computers, the protocol the data package uses is SMB2
5. Detect unwanted dhcp servers. even though in the office the network is set to static, it turns out that there is an active dhcp server. The dhcp server broadcast data will be visible on Wireshark.

6. Can detect ARP Poisoning and ARP Spoofing, which means someone is messing with the ARP table (usually someone is running Man in The Middle Attack)

Wireshark itself also has quite complete features, including:
1. Multiplatform, can be used for several base operating systems (Unix, Mac, Windows, and Linux)
2. Capture network data packets in real time
3. Can display network protocol information from data packets completely
4. Data packages can be saved as files and later can be reopened for further analysis
5. Filtering network data packets
6. Search data packages with specific requirements
7. Data packet appearance coloring to facilitate packet data analysis
8. Display statistical data.

To capture incoming and outgoing data packets on the network, Wireshark requires a physical NIC (Network Interface Card) device.

To use this tool is not that difficult, just enter the command to get the information you want to get from the network. Broadly speaking, how the wireshark works consists of two stages, namely:
1. Record all packets that pass through the selected interface (Interface is a connecting device between networks, can be via wifi or ethernet / lan card).
2. The results of these recordings can be analyzed. Can filter what protocols you want such as tcp, http, udp and so on. Wireshark can also record cookies, posts and requests.
3. Packages recorded by wireshark are packages that go through the interface only. That is why you cannot record your friend's data packet next to it even though they are both connected on the same network. This happens very often because many don't know how wiresharks work.
4. If you run Wireshark at the same time you open a browser on your own computer, the data can be captured completely. This is because the data is certain through the interface. So once again the package is stored only if it goes through the specified interface.

2.4 Accounting Information System

Meanwhile, according to Romnet and Steinbart, SIA is a system that collects, records, stores, and processes data into useful information in helping the decision-making process. In conclusion, the accounting information system means a system that includes records, forms, and reports with a certain arrangement so as to produce the financial information the company needs.

So, management can more easily control the work of the system that has been used. In the past, accounting records used the manual method. Currently, accounting information systems are easier to design because they can be created automatically.

There are five basic principles which have urgency on the reliability of the AIS system. These five principles are formulated by the AICPA or the American Institute of CPA. Here's the full review:
1. Security where access to the system and its data is controlled and is also limited to those who are authorized.
2. Confidentiality is the protection of sensitive information from unauthorized disclosure.
3. Privacy, which is the collection, disclosure, and use of personal information about customers in a more private and appropriate way.
4. Processing integrity where data processing is complete, accurate, timely, and also carried out with proper authorization.
5. Availability where the accounting information system is available for the fulfillment of operational obligations in accordance with the contract.

Running a system is not always smooth, there will be obstacles to overcome. In running an accounting information system, there are several common obstacles that often occur, including:
1. Companies need accounting software and computer equipment that can support one hundred percent security and confidentiality of financial data.
2. There are human resources who are not ready to implement the new financial system and standardization. So it takes more time in training and application.
3. Incomplete financial data and information generated. So, there is still a verification process. The time needed is even longer than it should be.

3. Method

The descriptive approach was adopted in this study through a collection of previous literature on Wireshark Packet Capture. Based on the literature review described, this study tries to explain how Wireshark Packet Capture is seen from the perspective of accounting information technology systems. The purpose of this paper is to show readers what Wireshark Packet Capture is from the perspective of accounting information systems itself.

4. Result and Discussion

4.1. Result

Technological developments are used to facilitate the flow of information in all areas of life, including business. The information network shortens and brings the distance between producers to consumers so that it is believed to be able to reduce barriers and increase business. In addition to having great benefits, the use of information networks needs serious attention because it can cause data leakage and not provide benefits and benefits but benefits.

Information technology is one of which is used in the field of accounting, namely management can more easily control the work of the system that has been used through the use of technology so that the accounting process can be carried out automatically, accurately and briefly.

The AICPA or the American Institute of CPA has formulated the reliability of the AIS system as follows:
1. Security where access to the system and its data is controlled and is also limited to those who are authorized.
2. Confidentiality is the protection of sensitive information from unauthorized disclosure.
3. Privacy, which is the collection, disclosure, and use of personal information about customers in a more private and appropriate way.
4. Processing integrity where data processing is complete, accurate, timely, and also carried out with proper authorization.
5. Availability where the accounting information system is

available for the fulfillment of operational obligations in accordance with the contract.

In addition to saving time, information technology for accounting must be able to provide security, confidentiality, privacy and integrity, while data leakage is one of the weaknesses of information technology. For that we need a wireshark application that can identify data leaks and maintain data security and confidentiality.

The Wireshark application itself is one of the Network Analyzer tools, aka a complete network protocol analyzer. commonly used by Network Administrators network problem solving, analysis, software and communication protocol development, and education. This program can record all passing packages and select and display the data in as much detail as possible, for example posting comments on blogs or even Username and Password.

The main Wireshark application functions are quite a lot. However, strangely this program is mostly known not for its main function but because it is often used for beginner hacking purposes.

Actually Wireshark is not designed for hacking / hackers. The main function of the Wireshark application is not intended for hacking. The main function of the Wireshark application is as a Network Administrator to be able to track what is happening in his network or to make sure the network is working properly, and no one does bad things on the network. The main function of the Wireshark application is used to perform network analysis and troubleshooter. This makes it possible to find out what problems occur on the network. Wireshark is a network analyzer program that is very popular today.

4.2 Discussion

Based on the research results above, the researcher will discuss the results of the above research as follows:

Along with the development of the world that is increasingly rapid, information is very useful for every life, especially in business or business activities. However some groups like hackers. That will steal all valuable information for the company. Wireshark is useful for network administrators even against Hackers as follows:

1. Loopback network, in a wirehark you can find an unreasonable number of packets due to network loops, for example, suddenly there are thousands of packets in seconds.
2. Detect problematic http packets (usually not reaching the server) by looking at the black packet.
3. Malware that continuously sends data, in this case we can see an IP ip that feels foreign, for example during breaks and no one accesses the computer but it turns out that the computer is sending data to a suspicious address.
4. WireShark can also see activities such as copying files that have been shared by other computers, the protocol the data package uses is SMB2
5. Detect unwanted dhcp servers. even though in the office the network is set to static, it turns out that there is an active dhcp server. The dhcp server broadcast data will be visible on Wireshark.
6. Can detect ARP Poisoning and ARP Spoofing, which means someone is messing with the ARP table (usually someone is running Man in The Middle Attack)

5. Conclusion

In this research, we see that the development of real information technology is very beneficial for every area of life, especially business, including in preparing financial reports by accountants.

At this time, the role of accountants is getting better if they are supported by expertise in the field information technology systems, so it is necessary to understand the use and evaluation of computer networks. Therefore accountants must also understand well information technology (IT), including its capabilities and risks.

A deeper understanding will help improve the expertise in using information technology to achieve supervisory goals in the organization. Maintain and control sources of information should be the top priority for management. To protect information sources from leaks that can cause harm, the wireshark application provides an answer, because in addition to early identification, its feature can also protect information sources from hackers.

6. References

1. Akbar, Sonhaji M. Network Analysis Using the Computer Network Wireshark Program, (Online), 2013, (http://msonson.blogspot.com/2013/04/analisa-jaringanmenggunakan-program.html).
2. Ariyanus. Instrusion Detection System, Andi: Yogyakarta, 2007.
3. Kumar M, Yadav R. TCP & UDP Packet Analysis Using Wireshark. Journal International Research in Science, Engineering and Technology Research. 2015; 4:1-5.
4. Kurniawan, Agus. How to Use Wireshark,(Online), 2014, (http://blog.aguskurniawan.net/post/Cara-Menggunakan-Wireshark.aspx).
5. Putra EM, Tujni B, Negara ES. Internet Network Security Analysis (WIFI) From Sniffing Data Packet Attacks At Muhammad University. Journal Universitas Bina Darma, 1-11.
6. Jogiyanto Management information System, 2009.
7. Susianto D, Rachmawati A. Network Implementation and Analysis Using Wireshark, Cain and Abels, Network Minner. Journal of Informatics Management. 2018; 16:1-6.