A Study of Packet Sniffing as an Imperative Security Solution in Cybersecurity

Abstract: This study aims to do deep research on packet sniffing activity and its importance to cyber security. The reason for the act of packet sniffing is when there are any errors or problems that requires troubleshoot. This includes errors regarding network error, malicious activities, unencrypted traffic, and many other issues. Therefore, the objective for this research is to monitor the network as well as analyzing any recorded data. Using packet sniffer, administrators are able to detect any malicious activities on the network. It is also a great way to study how the network operates and understand the network protocols. In this research, readers will discover many features of packet analyzer and learn their functions. There is also a technical demonstration activity where packet sniffer program will be used to capture packets from certain interface to collect data. The data recorded will be analyzed later on and will be discussed. The packet sniffing activity is focusing on network security at the third layer of OSI model. From this research, people can acknowledge the importance of packet sniffing activity, while hackers may use it for bad intention, is an excellent tool for administrators to monitor malicious activities on their networks.

Keywords: Packet sniffing, Packet analyzer, Wireshark, Packet capture, Network monitoring

1.0 INTRODUCTION

Packet sniffing is an act of monitoring packets flowing through a certain network [1]. Packets is basically data that is transmitted through computer network. From the sender, the data will be broken down into packets and reassembled at receiver. Every packet can be collected and then further analyzed using packet analyzer.

Packet analyzer is a computer program that capable of performing the packet sniffing activity. It can obstruct and log traffic that pass through the network. The process is called packet capture. As the data flows across the network, packet analyzer can capture every single one of data packets and decodes them, analyzes and revealing the content. There are various types of packet analyzer available to use, but the one to choose is Wireshark. Wireshark, which previously named Ethereal, is a free packet analyzer. It is easy to use, globally accessible and one of the most popular network analyzer tools [2]. There are many functions and capabilities of Wireshark. Network problems can be analyzed and troubleshoot including latency issues, dropped packets and malicious activity across the network. Network intrusion and misuse can be detected while analyzing packets. By tracking down the IP address, whatever unwanted application can be blocked by stopping it from sending or receiving packets.

The first ever packet sniffer device was called Novell LANalyser [3]. It can capture packets which then enables it to observe the population of network segmentation. It could also analyze problems in detail at network server. Throughout the years, network admins used packet sniffing tools to observe networks, perform analysis and troubleshoot problems. Packet sniffing was initially meant to be used as a diagnostic tool to keep data and other information being sent within the network. As technologies advanced over time, new devices and programs have developed too. The revolution of packet sniffing to become useful tool for business and companies is very important in the security world. However, these programs began to utilize their techniques in a bad way where they attack the computer networks and deploy schemes to acquire data information that should have been kept secure.

2.0 LITERATURE REVIEW

Asrodia, Pallavi and Patel [4] discusses on basics of packet sniffer, its operation, and several packet sniffing tools, as well as their capabilities for monitoring and analysis of network. They defined packet sniffing as a

method of monitoring packets across the network. It is operated by a packet sniffer which is either software or hardware. Packet sniffing is passive in nature, making it impossible to detect. The packets captured can be saved for later analysis. They concluded that while there are many tools intended to capture network traffic, some of them cannot be analyzed, have large memory requirement, and some of them even limited only to trace IP packets.

Similarly, Ben-Eid [5] explores packet sniffer definition, structure, types and its functions. Two of the which are Wireshark and Colasoft Capsa are the most popular selection packet sniffing software that will be examined thoroughly. They compared together both software based on their characteristics and other different parameters. Information technology improves worker effectiveness despite having negative repercussion. Worker often uses the Internet at their workstation for their personal interest. This will result in affecting the performance of the network and, in consequence, reduce level of productivity of worker. They study the problem of Internet usage by these employees in order to stay away from any computer abuse in the organization.

Oluwabukola, Oludele, and Ogbonna [6] developed the implementation of a Psniffer application that captures data packets and later provides reasonable means for decision making process. The application which was developed in Java has features similar to existing packet sniffer program such as monitoring network

Sikos [7] in his article, talks about the practice of packet analysis and deep packet inspection in network forensics. Advanced network traffic classification and pattern identification capabilities included in AI powered packet analysis method were reviewed. Types of digital evidence that are admissible will be discussed since not all evidence can be brought up to the court. Potential use of hardware appliances and packet analyzer software

Kulshrestha and Dubey [8] discusses about type of sniffing attacks, sniffing tools and techniques, online adaptation, and other related techniques. Security measures and overcoming issues of sniffing attacks will also be reviewed. Privacy of data and information stored on web is normally underestimated by users as is it easy for anyone to access. Confidentiality is an important part of network security to prevent any unauthorized access. This includes the use of passwords to access information. Trust that the data will remain the same and not be modified symbolizes integrity. Availability may be affected by computer break down or crash which may question the availability of information to the authorized user. They also review on security measures applied between client and server during information flow.

3.0 METHODOLOGY

Steps and techniques to utilize packet sniffer were revised. Technical demonstration was conducted in real life environment to get the experience of using packet sniffer program and analyze all the data recorded. Appropriate packet sniffer software needs to be download in order to perform the activity, where in this project uses Wireshark.

3.1 Block Diagram

Packet sniffer was placed at the client where it will intercept any data that flows through between client and the server as shown in Figure 1. It can save all the packets captured with a program called Pcap which enables user to see and analyze the packets even during offline mode.

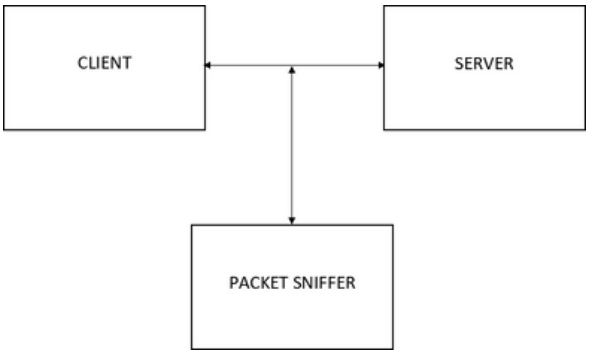

Figure 1: Block Diagram

3.2 Flowchart

The flowchart in Figure 2 explains step by step including preparation before packet capture. To start the demonstration activity, the steps will start with sketching the network diagram based on the environment chosen. The reason of this is to visualize how the network operates and get a clear view of all the connections between

equipment. Next is to set up the equipment according to the sketch network diagram. Make sure to use appropriate cable and check if all connections are successful. After setting up is done, packet sniffing activity can start by launching packet sniffer program. Starting from this step, it is depending on the packet sniffer program software itself. Different program offers different steps, but the objective and result are still the same. Normally, the program has options to choose interface at which packets want to be captured. After finishing packet capture, simply stop the process and result of data will be available. All these data will later be analyzed. As there are so many traffics that flows through the network, filter feature can be used to narrow the search on specific protocol.

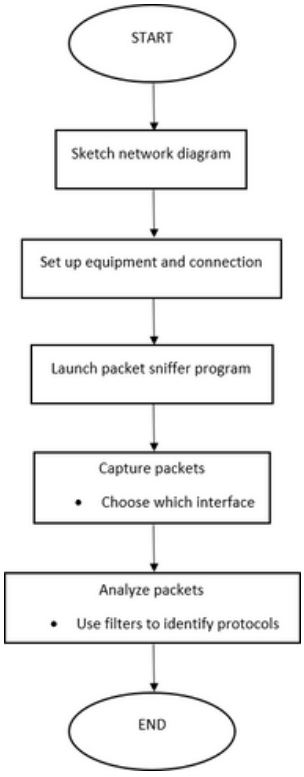

Figure 2: Flowchart

3.3 About Wireshark

Wireshark can be used by anyone whether for good or bad intention. Such packet analyzer can be used to troubleshoot networking issues, record communications (e.g., email, voice, chat), record and analyze web traffic, reconstruct image, and even capture usernames, passwords, or any personal information throughout the traffic. Data flows in a form of packets. A single packet contains source and destination IP address and ports, MAC address, Time To Live (TTL), protocols file. Pcap file is commonly used in other packet analyzers including Wireshark.

Figure 3 shows that user interface of Wireshark can be separated into four parts. Main toolbar has the options to capture packets, find packets, filter packets and other useful tools. Packet list pane is a tabular view of packets in pcap file which are being captured in real time. By interpreting data in this pane enables user to, under certain circumstances, troubleshoot network problem without having to perform a detailed audit. Packet details pane shows the different layers of the OSI model. This is the part where user can drill deeper and navigate into different pieces of a packet. When highlighting certain parts in packet details, the corresponding raw details will be highlighted in the Packet bytes pane which shows the binary data of the packet.

Figure 3: Wireshark User Interface

GeoIP mapping is an additional feature of Wireshark. It has the capability to plot endpoints on a trace file on a map of the world. It uses the MaxMind GeoLite2 databases that includes information such as location of the city, country and Autonomous System Number (ASN) [9].

3.4Technical Demonstration

In order to get a clearer view on packet sniffing, technical demonstration was conducted using real life environment. Figure 4 below shows the network diagram where laptop has wireless connection to the router where Internet is provided. Packet sniffer program chosen for this demonstration is Wireshark and is installed to the laptop.

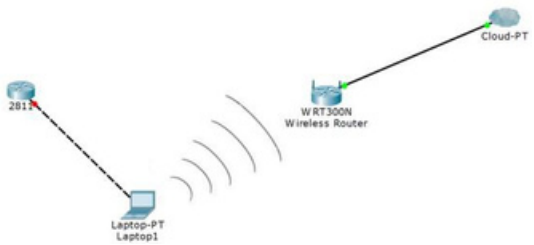

Figure 4: Network Diagram

First step is to connect the client to Wi-Fi to establish Internet connectivity. The next step is to launch Wireshark. Double click the Wi-Fi interface to start capture packets. While capturing packets, user can start browsing the Internet where any network traffic will be captured as well. Start by browsing techpanda.org. It is a simple login website with password. Second website to browse is dalberghetti.com. It is a website with only one photo displayed. Next website to be browsed is intra.unikl.edu.my. For the last sample, browse sportonly.com which will result in an error since the site cannot be reached. After finish browsing all the four sample websites, open Wireshark and stop capture. Save the capture file for easier analysis. The saved file will have extension of pcapng.

4.0 RESULTS

Now that the captured file is already saved, user can open the captured file to be analyzed. Analyzation of packets was done to the captured traffic on how to read the packets and how to retrieve any information based on the sample website browsed during capture using Wireshark. Figure 5 below shows the captured file of the demo.

Figure 5: Captured file

4.1 Statistical Data

The Statistics menu in Wireshark allows access to a wide range of network statistics. These statistics include everything from general information about the loaded capture file to statistics about specific protocols.

From Capture File Properties, several parameters can be obtained such as File, Time, Capture, Interfaces, and Statistics. Timestamps shows the first and last packet including their difference shown at elapsed where it was 1 minute and 26 seconds long. The measurement of the captured file is a total of 3587 packets, time span of 86.322 seconds, 2311933 bytes, with an average of 26k bytes/s.

Protocol Hierarchy collects data about the protocol distribution in the captured file [10]. Calculation of data regarding packets, bytes and bit/s are shown in the window. There are also End Packets, End Bytes and End Bits/s columns where it stated the absolute amount of data where it was the highest protocol in the stack.

A network endpoint is the logical endpoint of certain protocol traffic of a certain protocol layer. Endpoints window has a tab for each protocol that is supported such as Ethernet, IPv4, IPv6, TCP, and UDP.

I/O Graphs window includes a chart drawing space, as well as a collection of graphs that can be customized. It shows how traffic flows across a network. The graphs are broken down into time intervals that can be set up. Associated packet in the packet list can be accessed by clicking on the graph. The default I/O graph will display a line graph which represents packets per second over time. At 64th second, it has the highest number of packets per second which is 720 packets as shown in Figure 6.

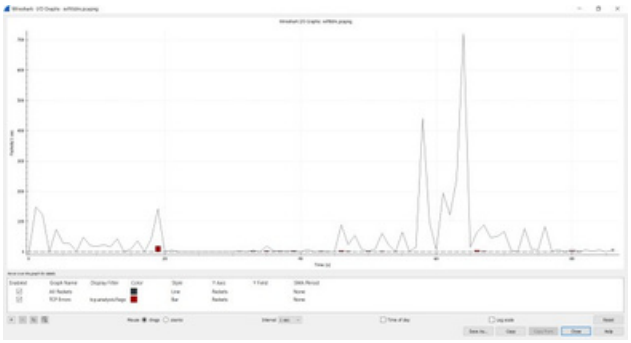

Figure 6: I/O Graph

4.2 Case 1

For the first case, is to retrieve username and password that were login previously at website techpanda.org. Wireshark cannot filter by website name; therefore, IP address of the website is required. One of the ways to find the IP address is to open Command Prompt on PC and use tracert command. Now that the IP address of the website was found, use the filter feature on Wireshark to find only the packets that flows through it. Type in “ip.addr ==” follows by the website IP address. Look for HTTP protocol and the word POST at info column and click on the packet. At the packet details pane, expand the information of HTML Form URL Encoded. This will show the email and password that were used to login to the page as shown in Figure 7.

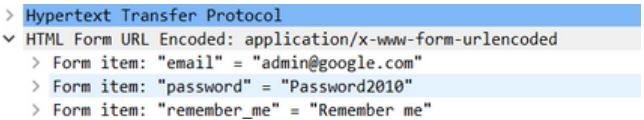

Figure 7: Login information retrieved

4.3 Case 2

For the next analysis, is to extract picture from the website dalberghetti.com. Similar to Case 1, it requires to find the IP address of the website using tracert command. Type in “ip.addr ==” follows by the website IP address at the Wireshark filter and analyze the packets. Look for any packet that contains JPEG file at the information column. Click on the packet and pay attention to the packet details pane. Right click on “JPEG File Interchange Format” line and choose “Export Packet Bytes…”. Save the file using extension .jpg to any folder in computer. Figure 8 shows the file that has been saved and its folder destination.

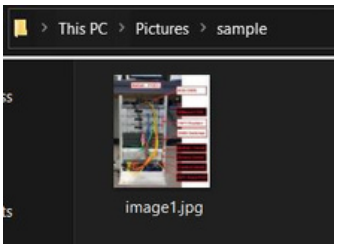

Figure 8: Picture extracted

4.4 Case 3

TLS handshake takes place whenever a user navigates to a website over HTTPS and the browser first begins to query the website's origin server. A TLS handshake also happens whenever any other communications use HTTPS, including API calls and DNS over HTTPS queries [11]. Comparing Figure 9; sequence of TLS handshake and Figure 10; packets captured, it was clear how TLS handshake works step by step at Wireshark.

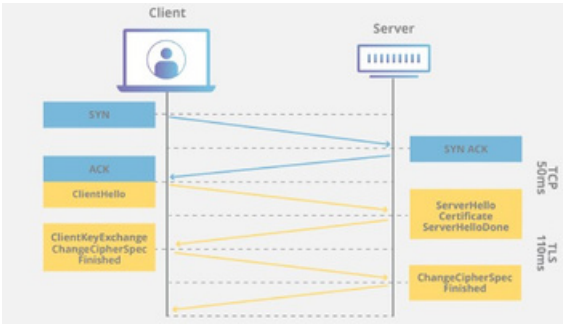

Figure 9: TLS handshake

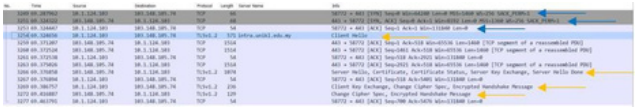

Figure 10: Packets filtered for intra.unikl.edu.my

4.5 Case 4

When a certain website is down, it will send synchronized TCP packets, but the result would be no answer. So, it keeps on trying to retransmit the TCP packets several times. This problem only occurs when trying to surf this website, not the entire network, since the website is down. All the process can be seen at Figure 11.

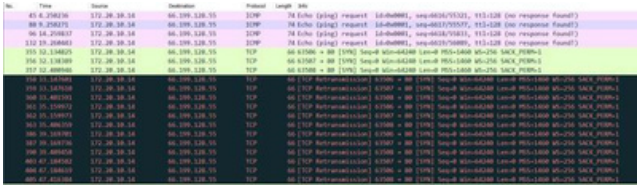

Figure 11: Packets filtered for sportonly.com

5.0 CONCLUSION

Analyzing network packets through the act of packet sniffing is a crucial way to monitor network traffic, troubleshooting, and collecting evidence for network forensic purposes. Wireshark is one of the most popular packet analyzer capable of performing packet sniffing. This packet sniffer contains many features that are easy to use, user friendly, efficient, and provide accurate data of the packets captured. Technical demonstration was done to present a clear view of real time packet capture during browsing sample websites. It evident that Wireshark has the ability to decrypt HTTP traffic, extract picture from raw data, observe TLS handshake of HTTPS traffic, and troubleshoot website down. Filtering features are vital as there are thousands of packets transmitted during capture. Suggestion for future research is to decrypt HTTPS traffic which may involve