IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Comparative Study on Packet Sniffing Tools

Miss. Shraddha Dilip Sarve[1] and Prof. Shubhangi Mahadik[2]
Student, Master in Computer Application[1]
Assistant Professor, Master in Computer Application[2]
Bharati Vidyapeeth, Navi Mumbai, Maharashtra, India

Abstract: *With the advancement and widespread use of network technology, network administration, maintenance, andmonitoring have become increasingly important in order tomaintain the network running smoothly and increase economic efficiency. A packet sniffer is used for this purpose. Network monitoring relies on packet sniffing to troubleshoot and log issues. Both network software engineers and network administrators will gain from network activity. There are a few variety of packet sniffers on the market that can be used to do packet sniffing. The subject of this paper is the fundamentals of apacket sniffer; its operating principle; and the numerous packetsniffing tools and how they work, network monitoring and analysis capabilities.*

Keywords: Packet capture, Network Monitoring, Packet sniffer, Wireshark, Tcpdump.

I. INTRODUCTION

A. Packet Sniffer

Packet sniffing is a network monitoring technique thatmonitors every packet that passes across it. A packet sniffer is a software or hardware device that monitors all network communication. This unlike traditional network hosts, which simply receive traffic, sent to them specifically the threat to security posed by the ability of sniffers to gather all incoming and outgoing data traffic, such as passwords and usernames in clear text, or other sensitive information It is theoretically impossible to detect. Because these sniffing instruments are passive in nature, they can be used in a variety of situations. They merely collect data, in other words. While they canbe fully utilized but some are not passive, thus they can be detected. Packet sniffer is a computer software that runs ona networked device. That passively collects all frames going through the data link layer through means of the device's

Fig. Packet Sniffing

II. WORKING

When a computer delivers data over the network, it doesso in packets. These packets are the data pieces that are truly directed to a certain system. In reality, every piece of data conveyed has a predetermined destination. As a result, all data is directed to a single computer. In most cases, a network system is designed to receive and transmit data. The packet sniffing procedure entails a collaborative effort between the two parties to read just the data that is intended for it. Both software and hardware are involved. The procedure can be divided into two parts. There are three steps. 1. A packet sniffer captures binary data from the cable in its raw form. This is usually accomplished by turning on promiscuousmode on the selected network interface. 2. Binary data is captured and transformed to a usable format. 3. Analyze the data that has been recorded and converted. The packet sniffertakes the network data it has recorded, verifies its protocol using the information it has gathered, and then begins its analysis of the protocol's unique characteristics. The first component of sniffer is packet capture. The packet capture library receives a copy of every link-layer frame that is sent from or received by your computer. The second component of a packet sniffer is the packet analyzer, which displaysthe contents of all fields within a protocol message. When a packet is sent, it will be transmitted to all available machineson local network.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

Owing to the shared principle of Ethernet, all computers on a local network share the same wire, so in normal situation, all machines on network can see the traffic passing through but will be unresponsive to those packets donot belong to themselves by just ignoring. However, if the network interface of a machine is in promiscuous mode, the NIC of this machine can take over all packets and a frameit receives on network, namely this machine (involving its software) is a sniffer [1]. Different types of network sniffing tools are available in the market, depending on the network, application, or protocol. This presentation examines the most important and practical aspects of Wireshark, tcpdump, and Soft Perfect Network are examples of packet sniffers, protocol analyzer, and so on.

III. WIRESHARK

Wireshark is a packet analyzer. It is used for network troubleshooting, analysis. Originally named Ethereal, in May2006 the project was renamed Wireshark due to trademark issues. Wireshark is cross-platform, using pcap to capture packets; it runs on various Unix-like operating systems and Solaris, and on Microsoft Windows. Wireshark allows the user to put the network interfaces that support promiscuous mode into that mode, in order to see all traffic visible onthat interface, not just traffic addressed to one of the in- terface's configured addresses and broadcast/multicast traffic[2]. When using a packet analyzer in promiscuous mode ona network switch port, however, not all of the traffic passing through the switch will be captured, be dispatched to the portwhere the capture is taking place ,capturing in promiscuous mode isn't always the best option ,but it sufficient to monitorevery network traffic. Wireshark is a programmed that allows you to see what is going on that "understands" the structure of various types of documents protocols for networking As a result, it is able to show the encapsulation, as well as the fields and their meanings a variety of packets defined by several networking protocols. Fig. 1 show wireshark tool.

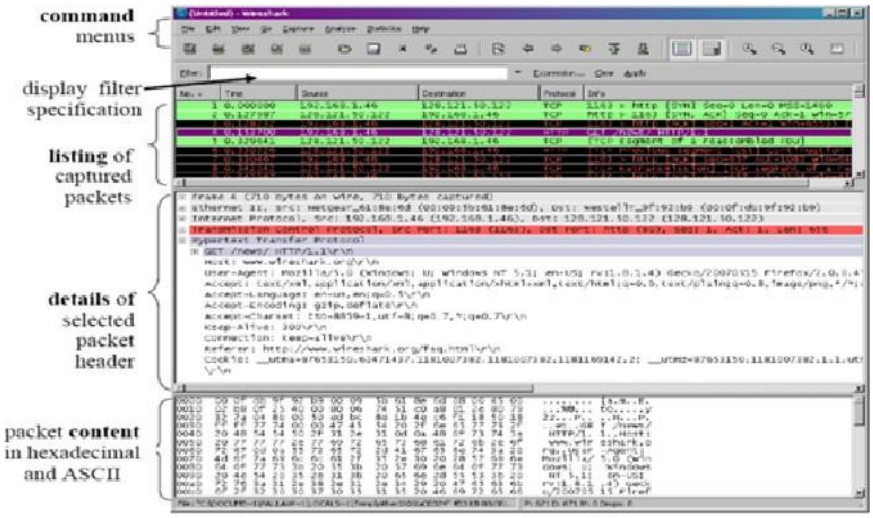


Figure 8: Wireshark Graphical User Interface on Microsoft Windows

Wireshark allows users to capture packets as they move across the whole network on a specific interface at a certain time. The is one of the most important tools. This is a toolfor capturing users can use the "Capture" menu to capture images. It can capture packets and offers a variety of choicesin order to meet the analysts' settings and conditions. Keep inmind as you go through the process of capturing the packagesAnalysts could even use filters to block out information that they don't want to see to capture unwelcome traffic.

IV. TCPDUMP

TCPdump is a tool that can be used to capture packets, monitor networks, and troubleshoot protocols. It is the oldestand most widely used command line utility that only works on the Windows operating system.Tcpdump writes out a description of the contents of data packets intercepted ona network on Linux-based platforms interface. Certain types of dumps can be added to this one ,it can be used to dump allnetwork traffic or it can be used to dump a subset of network traffic at the time when it was in use In addition to recordingand storing data, Tcpdump provides a number of options for

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

filtering received packets. functionalities: 1) read and write captured traffic to Packet Capture (PCAP) format data files, 2) filter packets based on parameters, and 3) print limitedor full data based on the criteria provided, information from each packet ,Tcpdump has certain basic settings that willbe used for network analysis while displaying the results on the screen to the data files. Tcpdump is a common packet analyzer that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Tcpdump works on most Unix-like operating systems: Linux, Solaris, BSD, and Mac OS. In those systems, tcpdump uses the libpcap library to capture packets. Theport of tcpdump for Windows is called WinDump; it uses WinPcap, the Windows port of libpcap. Tcpdump analyzes network behavior, performance and applications that generate or receive network traffic [3]. Tcpdump displays network traffic in its most basic form. By default, it publishes asummary of the packets intercepted on the wire, but it does not store the data included in those packets. More specific details can be provided if desired. It contains information such as the date and time of the capture, IP addresses in Domain Name System (DNS) addresses, and port numbers, among other things. The data is useful because it may be usedto figure out which machines were involved in connections, what general protocols (IP) were used, and when the packetswere captured. It does not, however, provide much relevant information on what a user is looking at and how that in- formation appears. Because Tcpdump uses the PCAP formatto directly export packets to the hard disc, the file contains much more detailed information; otherwise, Tcpdump only gives the packet headers and contents. Tcpdump's limitationsare that it gives information that is geared toward the technically savvy user. It does not provide a way for a userto read an entire data file, whether text-based or visually, in order to discover what data is contained within it. When the goal of network analysis is to determine and visualise the actual content of packets, this can limit its usefulness. [5].

V. SOFT PERFECT NETWORK PROTOCOL ANALYZER

Soft Perfect Network Protocol Analyzer is a sophisticated,professional tool for analysing, debugging, maintaining, and monitoring local and Internet networks. It collects data from your dial-up connection or network Ethernet card, analyses it,and then displays it in an easily understandable format. Net- work administrators, security specialists, network applicationdevelopers, and anybody else who wants a detailed viewof the traffic travelling through their network connection or portion of a local area network may find Soft Perfect Net- work Protocol Analyzer useful. The results of Soft Perfect

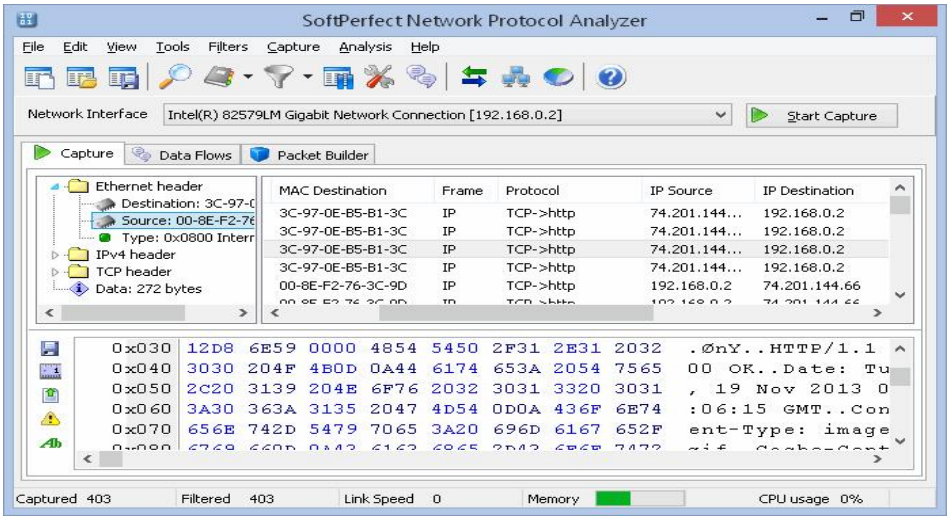
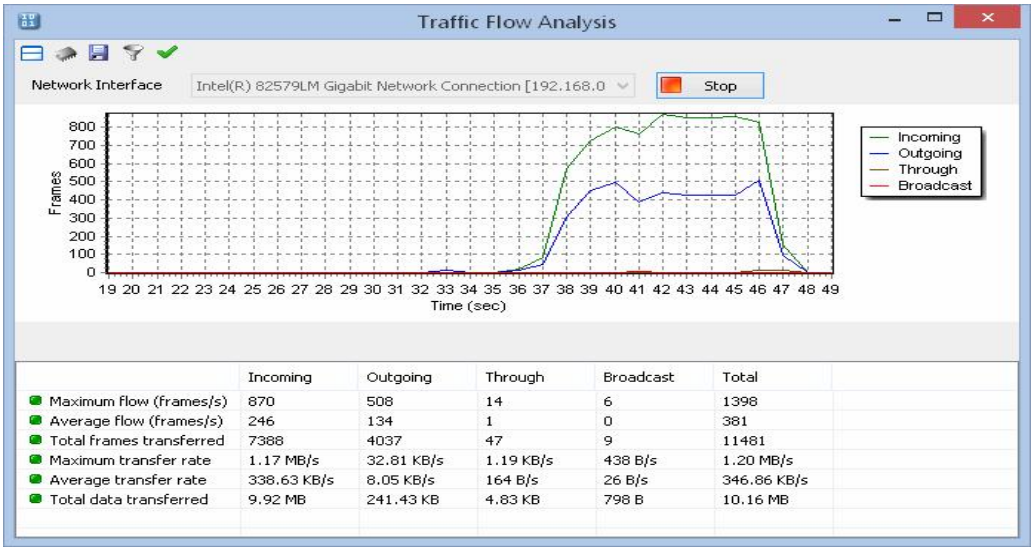


Fig. 2 Capture Packets

Network Protocol Analyzer's network analysis are presentedin a simple and easy-to-understand style. It also defrays and reassembles network packets into streams for you. The software can quickly examine network data using a variety of Internet protocols. This utility allows you to create and send your own unique network packets over the network. This packet builder feature could be used to test your network's security against attacks and intruders. The output of this tool is shown in Figures 2 and 3. However, this programmed is only compatible with the Windows operating system. [4].

Fig. 3 Packet Analysis Graph

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252



	Incoming	Outgoing	Through	Broadcast	Total
Maximum flow (frames/s)	870	508	14	6	1398
Average flow (frames/s)	246	134	1	0	381
Total frames transferred	7388	4037	47	9	11481
Maximum transfer rate	1.17 MB/s	32.81 KB/s	1.19 KB/s	438 B/s	1.20 MB/s
Average transfer rate	338.63 KB/s	8.05 KB/s	164 B/s	26 B/s	346.86 KB/s
Total data transferred	9.92 MB	241.43 KB	4.83 KB	798 B	10.16 MB

VI. DIFFERENCE

Tcpdump is a network sniffer and parsing command-line utility that has been ported to a variety of systems. Wireshark is comparable to tcpdump, except it has a graphical user interface and a lot of complex filtering and sorting features. TcpDump uses extremely little RAM, as its installation file is only 484 KB in size. TcpDump does not have a graphical user interface that is easy to use (GUI). As a result, the user must learn those commands and become familiar with the command prompt-like UI. The limitation is a major factor in why it isn't used. Wireshark, on the other hand, has a highly user-friendly GUI, but its installation file is 18 MB, and it will occupy 81 MB in Windows and 449 MB in Linux after installation. As a result, it is quite expensive in terms of memory requirements. Unlike the other Sniffers, which are written in C, the Psniffer is written in Java. The requirement for a platform agnostic (i.e., architecture neutral) language to produce software for embedding in various consumer electronic products was the driving force for the development of this language. Except for the limits imposed by the Internet environment, Java is a unified and consistent programming language that allows the programmer complete power. Finally, Java is equivalent to C in terms of Internet programming. It records the packet, its size, and the IP ad- dresses of the source and destination machines participating in the packet transfer. It depicts this process graphically, as well as the operation of many layers. It provides detailed information about the intercepted packets, such as the layers involved and the protocols in use at the time. Finally, it has a mechanism for storing packet information.

VII. CONCLUSION

A network monitoring tool is a packet sniffer. It's useful for network traffic monitoring, traffic analysis, and trou- bleshooting, among other things. There are various tech- niques accessible to capture network traffic that researchers employed in their research, however their work has a con- straint. Because some technologies merely capture network traffic without analyzing it, the researcher must use other tools for analysis in order to obtain the traffic features he requires for his job. Some programs necessitate a lot of RAM. Some tools are only capable of tracing IP packets, while others are only capable of capturing TCP packets. We can conclude from the following research that packet sniffers can be useful in intrusion detection. TCPdump over.

REFERENCES

[1]. Adeer M.A., Zahid M., Iqbal A., Siddiqui M.R "Network Traffic Analysis and Intrusion Detection Using Packet Sniffer"ICCSN'10 Second International Conference, (2010), Page(s): 313-317(2010).

[2]. Dabir, A. Matrawy, "Bottleneck Analysis of Traffic Monitoring Using Wireshark", 4th International Conference on Innovations in Information Technology, 2007, IEEE Innovations '07, 18-20 Nov. (2007), Page(s): 158-162(2007).

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 1, July 2022
Impact Factor 6.252

[3]. McCanne and V.Jacobson. "The BSD Packet Filter: New Architecture for User Level Packet Capture", USENIX Conference, January, Pages 259-270(1993)

[4]. About soft perfect network protocol analyzer [Online] Available http://www.softperfect.com/products/networksniffer/

[5]. About Tcpdump [Online] Available http:// www.tcpdump.org/.