International Journal of Electrical, Electronics and Computer Engineering **1**(1): 55-58(2012)

ISSN No. (Online) : 2277-2626

Analysis of Various Packet Sniffing Tools for Network Monitoring and Analysis

Pallavi Asrodia* and Hemlata Patel*

** Department of Computer Science and Engineering,*
Jawaharlal Institute of Technology, Borawan, Khargone, (M.P.)

(Recieved 15 April, 2012 Accepted 5 May, 2012)

ABSTRACT : With the development and popularization of network Technology, the management, maintenance and monitoring of network is Important to keep the network smooth and improve Economic efficiency. For this purpose packet sniffer is used. Packet sniffing is important in network monitoring to troubleshoot and to log network activities which will benefit both the network Software engineers and network administrators There are various packet sniffers are available in market by which we can perform packet sniffing. This paper focuses on the basics of packet sniffer; it's working Principle and various packets sniffing tools their working and their capabilities for network monitoring and analysis.

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

I. INTRODUCTION

Packet Sniffing is a technique of monitoring every packet that crosses the network. A packet sniffer is a piece of software or hardware that monitors all network traffic. This is unlike standard network hosts that only receive traffic sent specifically to them. The security threat presented by sniffers is their ability to capture all incoming and outgoing traffic, including clear-text passwords and usernames or other sensitive material. In theory, it's impossible to detect these sniffing tools because they are passive in nature, meaning that they only collect data. While they can be fully passive, some are not therefore they can be detected Packet sniffer is a program running in a network attached Device that passively receives all data link layer frames passing through the device's network adapter. It is also known as Network or Protocol Analyzer or Ethernet Sniffer. The packet sniffer captures the data that is addressed to other machines, saving it for later analysis. It can be used legitimately by a network or system administrator to monitor and troubleshoot network traffic [1].

II. WORKING

When a computer sends a data n the network it sends in the form of packets. These packets are the chunks of data are actually directed to the certain designated system. Actually every sent data has a predefined receiving point. So, all the data are directly directed to a particular computer. Normally a system in a network is designed to receive and read only those data which are intended for it, the packet-sniffing process involves a cooperative effort between software and hardware. Process can be broken down into three steps.

1. Packet sniffer collects raw binary data from the wire. Typically, this is done by switching the selected network interface into promiscuous mode

2. Captured binary data is converted into a readable form.

3. Analysis of the captured and converted data. The packet sniffer takes the captured network data, verifies its protocol based on the information extracted, and begins its analysis of that protocol's specific features [9].

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 displays the contents of all fields within a protocol message. When a packet is sent, it will be transmitted to all available machines on local network. 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 do not 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 frame it receives on network, namely this machine (involving its software) is a sniffer [2].

There are different types of network sniffing tools depending on the network, application or protocols are available in markets. This paper considers the primary and most useful packet sniffer like wireshark, tcpdump, Soft Perfect Network Protocol Analyzer etc.

III. WIRESHARK

Wireshark is a packet analyzer. It is used for network troubleshooting, analysis. Originally named Ethereal, in May 2006 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 on that interface, not just traffic addressed to one of the interface's configured addresses and broadcast/multicast traffic [3]. However, when capturing with a packet analyzer in promiscuous mode on a port on a network switch, not all of the traffic traveling through the switch will necessarily be sent to the port on which the capture is being done, so capturing in promiscuous mode will not necessarily be sufficient to see all traffic on the network. Wireshark is software that "understands" the structure of different networking protocols. Thus, it is able to display the encapsulation and the fields along with their meanings of different packets specified by different networking protocols Fig. 1 show wireshark tool.

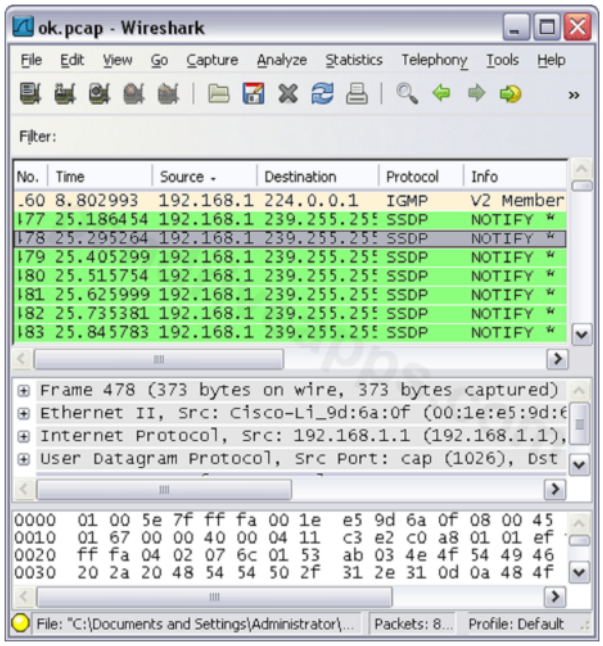

Fig. 1. Wireshark tool.

Wireshark provides users the capability of capturing the packets traveling over the entire network on a particular interface at a particular time. One of the primary tools is the capture tool. "Capture" menu is provided for the users to perform Packet Capture, and it also provides several options for suiting the situations and the conditions that the analysts have in the mind while performing the process of capturing the packets. Analysts could even set filters to avoid capturing unwanted traffic [11].

But wireshark have some limitation like Wireshark isn't an intrusion detection system. It will not warn you when someone does strange things on your network that he/she isn't allowed to do and Wireshark will not manipulate things on the network On the other hand Wireshark has a very good user friendly GUI. But its installation file size is 18 MB and after installation it will consume 81 MB in Windows and a hefty 449 MB in Linux [5].

IV. TCPDUMP

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. The port 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 [10]. It can also be used for analyzing the network infrastructure itself by determining whether all necessary routing is occurring properly, allowing the user to further isolate the source of a problem. It is also possible to use tcpdump for the specific purpose of intercepting and displaying the communications of another user or computer [11].

Tcpdump also have some limitations like- Tcpdump is also able to report on only what it finds in the packet. If an IP address is forged in the packet, tcpdump has no ability to report anything else and TcpDump is very economical in terms of memory because its installation file size is just 484 KB. TcpDump does not have a user friendly Graphical User Interface (GUI). So the user has to study those commands and get acquainted with the command prompt like screen. That limitation may play a key role in not choosing it for use [6].

V. SOFT PERFECT NETWORK PROTOCOL ANALYZER

Soft Perfect Network Protocol Analyzer is an advanced, professional tool for analyzing, debugging, maintaining and monitoring local networks and Internet connections. It captures the data passing through your dial-up connection or network Ethernet card, analyzes this data and then represents it in an easily readable form. Soft Perfect Network Protocol Analyzer is a useful tool for network administrators, security specialists, network application developers and anyone who needs a comprehensive picture of the traffic passing through their network connection or segment of a local area network. Soft Perfect Network Protocol Analyzer presents the results of its network analysis in a convenient and easily understandable format. It also allows you to defrayments and reassembles network packets into streams. The program can easily analyze network traffic based on a

number of different Internet protocols. Soft Perfect Network Protocol Analyzer also features a packet builder. This tool allows you to build your own custom network packets and send them into the network. You could use this packet builder feature to check your network for protection against attacks and intruders. Fig. 2 and 3 shows the result generated from this tool. But this tool only work for windows operating system [7].

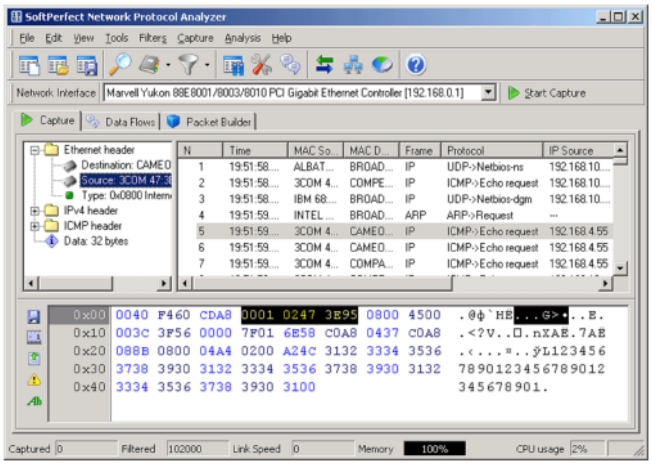

Fig. 2. Captured Packets.

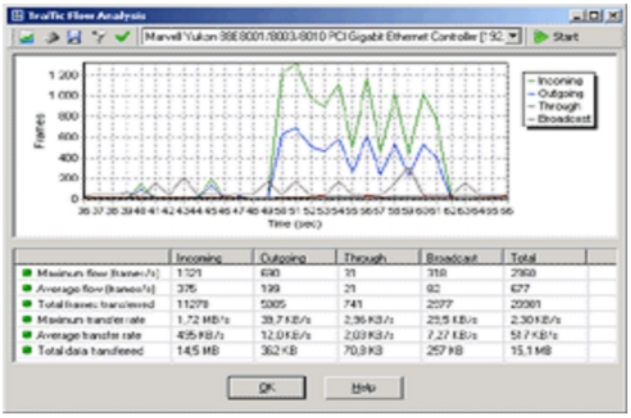

Fig. 3. Packet Analysis graph.

VI. CAPSA

Capsa is a network analyzer for both LAN and WLAN which performs real-time packet capturing, 24/7 network monitoring, advanced protocol analysis, in-depth packet decoding, and automatic expert diagnosis. It provides a comprehensive and high-level visibility to your entire network, helps network administrators or network engineers quickly pinpoint and resolve various application problems, and therefore enhance end user experience and guarantee a productive network environment. Identify and analyze more than 300 network protocols, as well as network applications based on the protocols; Monitor Internet, e-mail and instant messaging traffic, helping keep employee productivity to a maximum; Map out the details, including traffic, IP address, and MAC, of each host on the network, allowing for easy identification of each host and the traffic that passes through each; Visualize the entire network in an ellipse that shows the connections and traffic between each host [8] Fig. 4 shows working of capsa.

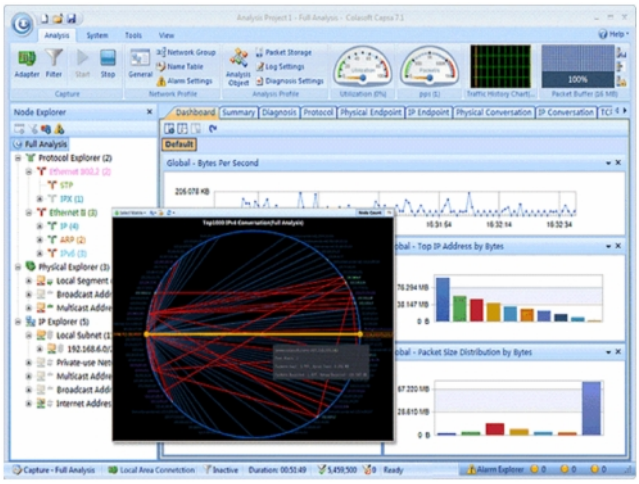

Fig. 4. Capsa tool.

VII. ETHERAPE

EtherApe is a packet sniffer/network traffic monitoring tool, developed for UNIX. Network traffic is displayed using a graphical interface. Each node represents a specific host. Links represent connections to hosts. Nodes and links are color coded to represent different protocols forming the various types of traffic on the network. Individual nodes and their connecting links grow and shrink in size with increases and decreases in network traffic [4]. Color coded node and links for most used protocols its basic functions are:

A. Traffic may be viewed on one's own network, end to end (IP) or port to port (TCP)

B. A variety of frame and packet types are supported.

C. Data view can be manipulated using a network filter.

D. Clicking a node or link provides additional information regarding including protocol and traffic information.

E. Can read traffic from a file or an actual network.

F. Handles traffic on Ethernet, WLAN, VLAN plus several other media and encapsulation types.

VIII. CONCLUSIONS

Packet sniffer is a network monitoring tool. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. There are many available tools used to capture network traffic that researcher used in their work, but there is a limitation in their work. Some tools only capture network traffic without analysis, therefore the researcher have to use another tools for

analysis to get the traffic feature like it is need in his work. Some tools have large memory requirement. Some tools only trace IP packets and some tools only capture tcp packets. By the following research we can conclude that packet sniffer can be used in intrusion detection.

REFERENCES

[1] S. Ansari, Rajeev S.G. and Chandrasekhar H.S., "Packet Sniffing: A Brief Introduction", *IEEE Potentials*, Dec 2002-Jan. 2003, Volume: **21** Issue: 5, pp: 17-19 (2002-2003).

[2] Qadeer 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).

[3] A. 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).

[4] All about Tools [Online] Available: http://www. sectools.org.

[5] All about Wireshark [Online] Available http:// www.wireshark.org/.

[6] All about Tcpdump [Online] Available http:// www.tcpdump.org/.

[7] All about soft perfect network protocol analyzer [Online] Available http://www.softperfect.com/products/networksniffer/

[8] All about capsa [Online] Available www.colasoft.com

[9] BoYu"Based on the network sniffer implement network monitoring Computer Application and System Modeling (ICCASM), 2010 *International Conference on Volume:* **7**, 2010, Page(s): V7-1-V7-3(2010).

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

[11] Dulal C. Kar Felix Fuentes. Ethereal vs. tcpdump: A comparative study on packet sniffing tools for educational purpose. *Journal of Computing Sciences in Colleges archive*, Volume **20**(4), pp 169-176, (2005).