ISSN: 2321-7782 (Online)
Volume 2, Issue 3, March 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Paper / Case Study
Available online at: www.ijarcsms.com

Signature Based Packet Sniffer

Ashish Kulkarni[1]
Dept. of Computer Engineering, P.V.P.I.T.
University of Pune
Pune – India

Nimish Kate[2]
Dept. of Computer Engineering, P.V.P.I.T.
University of Pune
Pune – India

Rohit Ghadshi[3]
Dept. of Computer Engineering, P.V.P.I.T.
University of Pune
Pune – India

Rushikesh Date[4]
Dept. of Computer Engineering, P.V.P.I.T.
University of Pune
Pune – India

Abstract: ***In the past five decades computer networks have kept up growing in size, complexity and, overall, in the number of its users as well as being in a permanent evolution. Hence the amount of network traffic flowing over their nodes has increased drastically. 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. Packet sniffers are useful for analyzing network traffic over wired or wireless networks. This paper focuses on the basics of packet sniffer; it's working Principle which used for analysis Network traffic.***

Keywords: Packet capture, Traffic analysis, Libpcap, Network Monitoring, NIC, Promiscuous mode, Berkeley Packet Filter, Network analyzer, Packet sniffer.

I. INTRODUCTION

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. Using the information captured by the packet sniffer an administrator can identify erroneous packets and use the data to pinpoint bottlenecks and help maintain efficient network data transmission. 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.

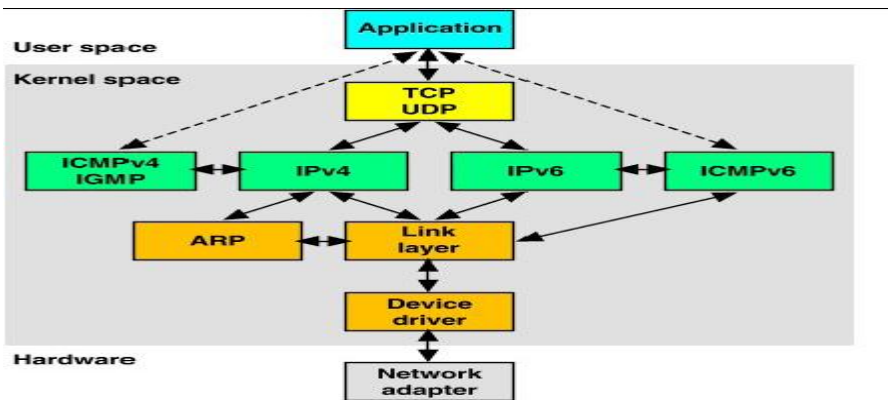

Fig. 1How packets travel from Application layer to NIC

II. WORKING

Each machine on a local network has its own hardware address which differs from other machines'. 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 [1]. When a packet is received by a NIC, it first compares the MAC address of the packet to its own. If the MAC address matches, it accepts the packet otherwise filters it. This is due to the network card discarding all the packets that do not contain its own MAC address, an operation mode called no promiscuous, which basically means that each network card is minding its own business and reading only the frames directed to it. In order to capture the packets, NIC has to be set in the promiscuous mode. Packet sniffers which do sniffing by setting the NIC card of its own system to promiscuous mode, and hence receives all packets even they are not intended for it. So, packet sniffer captures the packets by setting the NIC card into promiscuous mode the packet arriving at the NIC are copied to the device driver memory, which is then passed to the kernel.

III. PROMISCUOUS MODE

The network interface card works in 2 modes-non promiscuous mode and promiscuous mode. When a packet is received by a NIC, it first compares of the packet to its own. If the MAC address matches, it accepts the packet otherwise filters it. This is due to the network card discarding all the packets that do not contain its own MAC address, an operation mode called non Promiscuous, which basically means that each network card is minding its own business and reading only the frames directed to it. In order to capture the packets, NIC has to be set in the promiscuous mode. Packet sniffers which do sniffing by setting the NIC card of its own system to promiscuous mode, and hence receives all packets even they are not intended for it. So, packet sniffer captures the packets by setting the NIC card into promiscuous mode. To set a network card to promiscuous mode, all we have to do is issue a particular ioctl ( ) call to an open socket on that card and the packets are passed to the kernel. In figure we can see network interface card (NIC).

IV. TOOLS FOR TRAFFIC ANALYSIS

There are various tools for traffic analysis

A .Wireshark:

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. 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 on Microsoft Windows.

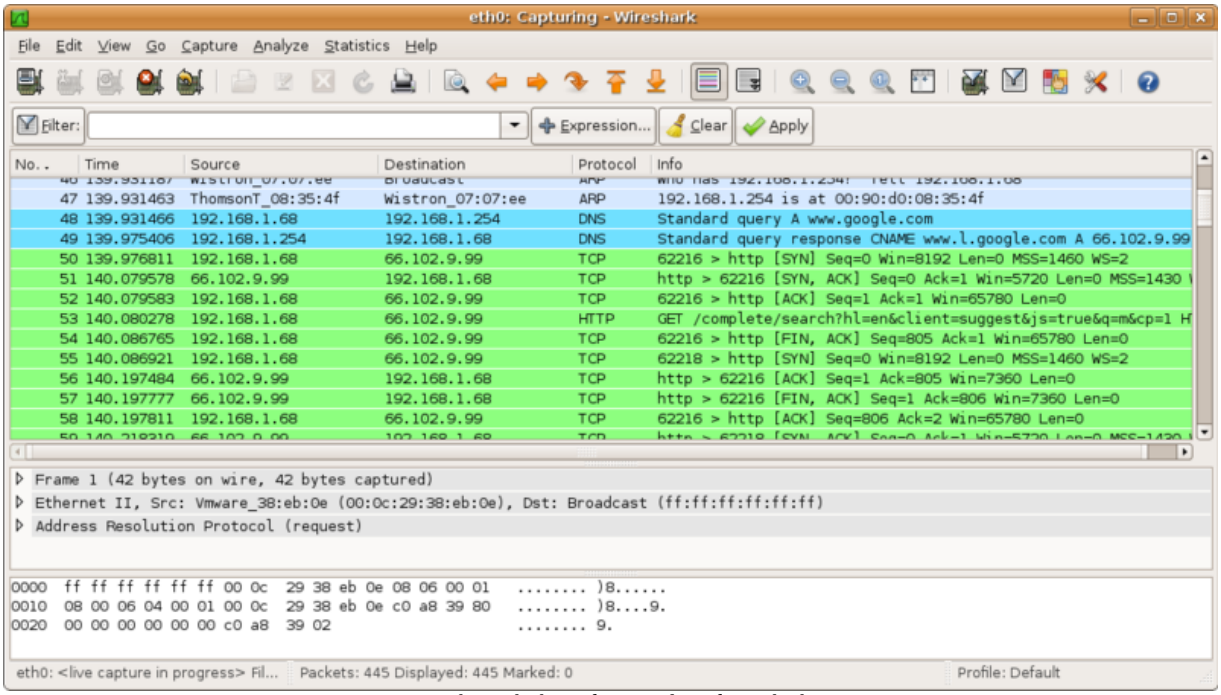

Fig 2.shows the basic functionality of wireshark.

B. Tcpdump:

It 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. Distributed under the BSD license, tcpdump is free software.Tcpdump works on most Unix-like operating systems: In those systems, tcpdump uses the libpcap library to capture packets. The port of tcpdump for Windows is called Win Dump; it uses WinPcap, the Windows port of libpcap.

C. Soft Perfect Network Protocol Analyzer:

It 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.

D. Capsa:

It is Network Analyzer is a must-have freeware for network administrators to monitor, troubleshoot and diagnose their network. It is designed for personal and small business use.Capsa Network Analyzer Free Edition is an easy-to-use Ethernet packet sniffer (network analyzer or network sniffer) for network monitoring and troubleshooting purposes. It performs real-time packet capturing, 24/7network monitoring, reliable network forensics, advanced protocol analyzing and in-depth packet decoding.

V. CONCLUSION

Packet sniffer can be enhanced in future with features like encryption and decryption options. A packetsniffer is not just a hacker's tool, network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. Packet sniffers can capture things like clear-text passwords and usernames or other sensitive material. 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. So we can design a tool that capture network traffic and analyze it and allows user to take only the feature as he need and store it in file to use it later in his work, then this will reduce the memory that is used to store the data. By the following research we can conclude that signature based packet sniffer is used for intelligent packet sniffing over the network.

References

1. Mohammed Abdul QadeerandMohammadZahid,"Network Traffic Analysis and Intrusion Detection using Packet Sniffer"2010.
2. Ryan Spangler "Packet Sniffing on Layer 2 Switched Local Area Networks" University of Wisconsin – Whitewater Department of Computer and Network Administration, Packetwatch Research URL: http://www.packetwatch.net (December 2003).
3. Suhas A Desai "Packet Sniffing: Sniffing Tools Detection Prevention Methods" University of California Department of Network Administration.(April 2004).
4. Ryan Spangler University of Wisconsin –"Packet Sniffer Detection with Anti Sniff" Research URL http://www.packetwatch.net (May 2003).
5. Capture Effect in IEEE 802.15.4 Networks:Modeling and Experimentation-Cengiz Gezer, Chiara Buratti, Roberto Verdone. WiLab - DEIS, University of Bologna.
6. Remote Sniffer Detection- David Wu and Frederick Wong fdavidwu , fredwongg@cs.berkeley.edu Computer Science Division University of California, Berkeley, CA 94720 (December 14, 1998).

