Pallavi Asrodia, Hemlata Patel / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.854-856

Network Traffic Analysis Using Packet Sniffer

Pallavi Asrodia*, Hemlata Patel**
*(Computer Science, dept., Jawaharlal Institute of Technology, Borawan, Khargone (M.P.) India.)
** (Computer Science, dept., Jawaharlal Institute of Technology, Borawan, Khargone (M.P.) 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 [2]. 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. In theory, it's impossible to detect these sniffing tools because they are passive in nature.

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 buffer from where it is used by the user application.

III SNIFFER COMPONENTS

Basic Components of sniffers are:-

A. The hardware: - Most products work from standard network adapters, though some require special hardware. If you use special hardware, you can analyze hardware faults like CRC errors, voltage problems, cable programs, "dribbles", "jitter", negotiation errors, and so forth

B.Capture driver:-This is the most important part. It captures the network traffic from the wire, filters it for the particular traffic you want, and then stores the data in a buffer.

C Buffer:-Once the frames are captured from the network, they are stored in a buffer.

D Decode: - this displays the contents of network traffic with descriptive text so that an analysis can figure out what is going on.

E Packet editing/transmission:-Some products contain features that allow you to edit your own network packets and transmit them onto the network

IV. IEEE 802.3 SNIFFING
In a typical IEEE 802.3 LAN network, a star topology is used, so all the nodes in the network are connected (through their own cable) to either a hub or a switch. Hubs are basically

repeaters: packets coming from a certain port are retransmitted over the rest of the ports. Switches instead, only send packets to the port where the destination host is connected, by previously identifying all the hosts connected to each port. Switched networks have Better performance than not switched networks. Switches may perform other actions over traffic, such as filtering based on different protocol fields (link, network, transport And application protocol fields, depending on the switch), That means that if a switched network is used, only packets flowing to or from the particular host running the sniffer or broadcast packets will be captured.

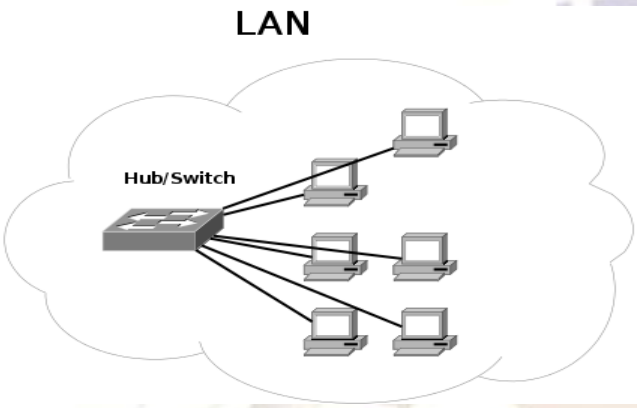

Figure 1: IEEE 802.3 networks

V. IEEE 802.11 SNIFFING

IEEE 802.11 based networks share access medium, so it may be easier than IEEE 802.3 switched networks to capture packets, as having a network card being able to be set to promiscuous mode (actually monitor mode) is all the hardware required. Nevertheless, some considerations have to be kept in mind. When placing a sniffer in a wireless network, some packets or even all the packets sent by a certain host may be lost, due to environment conditions (shadowing) and the physical position of the sniffer host and the other hosts in the network (attenuation due to propagation). IEEE 802.11 networks made up by several access points may increase capturing problems, due to the

Larger coverage area (and therefore the higher reception antenna gain needed when using a unique sniffer host).

VI. NETWORK TRAFFIC ANALYSIS

Network traffic analysis could be defined as: "the inference of information from observation of the network traffic data flow". Analysis in general, and hence network traffic analysis, can be categorized by time (or frequency) criteria and by the purpose of the analysis. Time based analysis categorization regarding time and frequency criteria, any network traffic analysis can be classified in one of the following three categories: real-time analysis, batched analysis and forensics analysis.

A. Real-time analysis: - It is performed over the data as it is obtained, or using small batches often called buffers to efficiently analyze data. The response time of this kind of analysis, understood as the time elapsed between a certain event occurs and is computed or detected, is low thanks to the low delay obtaining data and the fact that real-time analysis are fully automated. Real-time analysis though, has usually high computational resources requirements.

B. Batched analysis: - Batched analysis performs analysis periodically, where the period is enough to accumulate data in so-called data batches. Depending on the batching policies, the response time and associated computational resources requirements may be higher or lower, but in general they offer a higher response time and lower computational resources requirements than real-time analysis (although they require larger storage size).

C. Forensics analysis: Forensics analysis are analysis performed when a particular event occurs (triggered analysis). A typical example of forensics analysis is the analysis performed when an intrusion is detected to a particular host. This kind of analysis require that data had been previously stored to be analyzed, and may also require of human intervention.

Network data inspection techniques obtain information of network data by inspecting network header fields of each packet, compute them and produce outputs or results. Packet in which packets are decoded and presented in a human readable way. Network analyzers like tcpdump, Wireshark are some examples of packet Decoding applications.

VII. 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. [5]

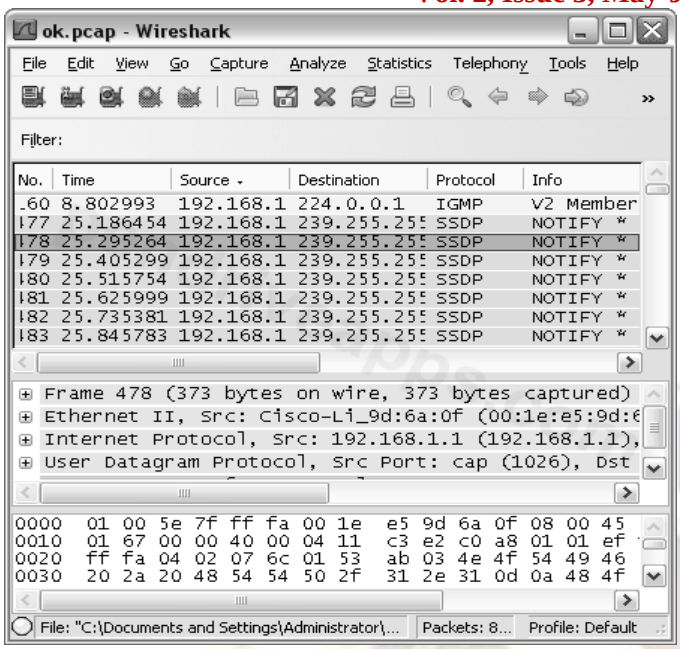

Figure 2: Wireshark Tool

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.

VIII. CONCLUSION

Packet sniffer is not just a hacker's tool. It can be used for network traffic monitoring, traffic analysis, troubleshooting and other useful purposes. When computers communicate over networks, they normally just listen to the traffic specifically for them. However, network cards have the ability to enter promiscuous mode, which allows them to listen to all network traffic regardless of if it's directed to them. Packet sniffers can capture things like clear-text passwords and usernames or other sensitive material. Sniffing is possible on non-switched and switched networks .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 packet sniffer can be used in intrusion detection.

REFERENCES

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

[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*

[3] G.Varghese, "Network Algorithmic: An Interdisciplinary Approach To Designing Fast Networked Devices*", San Francisco, CA: Morgan Kaufmann, 2005.*

[4] J. Cleary, S. Donnelly, I. Graham, "Design Principles for Accurate Passive Measurement," *in Proc. PAM 2000 Passive and Active Measurement Workshop (Apr. 2000).*

[5] 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*

[6] Bo Yu"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*

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